TATA INSTITUTE OF FUNDAMENTAL RESEARCH
STUDIES IN MATHEMATICS

General Editor : M. S. NARASIMHAN

1. M. Hervé : SEVERAL COMPLEX VARIABLES
2. M. F. Atiyah and others : DIFFERENTIAL ANALYSIS
3. B. Malgrange : IDEALS OF DIFFERENTIABLE FUNCTIONS
4. S. S. Abhyankar and others : ALGEBRAIC GEOMETRY
5. D. Mumford : ABELIAN VARIETIES

ABELIAN VARIETIES

DAVID MUMFORD

Published for the
TATA INSTITUTE OF FUNDAMENTAL RESEARCH, BOMBAY
OXFORD UNIVERSITY PRESS
1970

Oxford University Press, Ely House, London W 1

GLASGOW NEW YORK TORONTO MELBOURNE WELLINGTON
CAPE TOWN SALISBURY IBADAN NAIROBI DAR ES SALAAM LUSAKA
ADDIS ABABA BOMBAY CALCUTTA MADRAS KARACHI LAHORE DACCA
KUALA LUMPUR SINGAPORE HONG KONG TOKYO

Oxford House, Apollo Bunder, Bombay 1 BR

David MUMFORD, 1937

PRINTED IN INDIA

INTRODUCTION

THIS BOOK is based on a series of lectures delivered in the winter of 1967-68 at the Tata Institute of Fundamental Research. These lectures were subsequently written up, and improved in many ways, by C. P. Ramanujam. The present text is the result of a joint effort.

To write a thorough treatise on abelian varieties would be a formidable job. This book covers roughly half of the material that I think should be in a reasonably complete treatment. We have covered:

(i) the basic material developed in the books of Weil [W1] and Lang [L],

(ii) the techniques from the theory of schemes, developed by Cartier and Grothendieck, which have given us a clear picture of the situation in characteristic p,

(iii) the basic analytic theory developed in the book of Conforto [Co].

Unfortunately, my treatment of these topics is not as elementary as it could be, and quite possibly a student will find the subject more accessible if he reads the earlier treatments of the subject instead of or as well as mine. However, I have attempted to keep the discussion as simple as was compatible with the amount of material to be covered. In particular, I recommend Chapter 2 (which is independent of Chapter 1) as the easiest. Many of the techniques which are generalized in Chapter 3 to subtler scheme situations are treated here in a more transparent classical setting. Were the book to continue, the topics which I would have liked to treat would be :

I. Jacobians,

II. Abelian schemes: deformation theory and moduli,

III. The ring of modular forms and the global structure of the moduli space,

IV. The Dieudonné theory of the "fine" characteristic p structure,

V. Arithmetic theory: abelian schemes over local, global fields.

I don't believe the word "Jacobian" is ever used in this book. Rather stubbornly I wanted to prove that the theory of abelian varieties could be developed without the crutch of " reduction to Jacobians ". One of the main reasons this is possible is that I have used systematically the higher cohomology groups: I am especially fond of the proof of the main theorem of §8, which replaces Theorem 4, p. 99 of Lang [L]. But I have to admit that some people might feel Lang's argument is more geometric. For a treatment of Jacobians, the reader should look at Weil's and Lang's books: especially the very important Theorem 31, p. 117 of Weil, which Lang strangely omits. For abelian schemes, some of the basic facts can be found in my book, *Geometric Invariant Theory*, Ch. 6, [M1]. This area has been greatly clarified by recent work of Raynaud which should appear soon. The connection of modular forms with moduli spaces of abelian varieties can be found in Baily [B] and Shimura [Sh], as well as in their talks at the Boulder Summer Institute [B-M]. A purely algebro-geometric treatment of the "theta-null werte", which are special modular forms, is in my paper [M2]. It is interesting to ask whether further ties between the analytic and algebraic theories exist: e.g. an algebraic definition of the Eisenstein series as a section of a line bundle on the moduli space. For the Dieudonné theory, see Manin [Ma], Oort [O], the Séminaire Heidelberg-Strasbourg [D-G], Tate [T1], and the papers of Barsotti [Bt]. Among the vast literature on the arithmetic theory, let me only mention the Néron model [N] and the stable reduction theorem for this [G1], Kodaira [K], the Mordell-Weil theorem [L-N], the report of Cassels' [C], and Tate [T2].

Some of the material in this book is new and has not been published elsewhere. This includes the results of §16 on the index of a nondegenerate line bundle, and the results of §23 on the theta-groups

$\mathcal{G}(L)$ in the case where ϕ_L is not separable. Simplifications in §6, §13 and §16, the very elegant appendix to §4 characterizing abelian varieties as complete varieties X with arbitrary composition morphisms $X \times X \to X$ admitting a 2-sided identity, and the treatment in §21 of the local invariants of division algebras with involutions of the second kind are all due to C. P. Ramanujam. I want to thank C. P. Ramanujam for all his efforts and to thank the Tata Institute for the very pleasant and stimulating environment which encouraged these lectures. It is a pleasure to acknowledge the help of the very able staff of the Tata Institute, of the Fulbright foundation, of Mrs. Laura Schlesinger, and of the National Science Foundation.

CONTENTS

I

ANALYTIC THEORY

1. Complex Tori. We shall investigate in this chapter a compact connected complex Lie group X of dimension g, i.e. a compact connected complex manifold of dimension g with a group structure on the underlying set such that the maps $X \times X \to X$, $X \to X$ defined by $(x, y) \longmapsto x.y$ and $x \longmapsto x^{-1}$ are holomorphic. Let V be the tangent space to X at the identity point $e \in X$. V is a complex vector space. Recall that for *every* complex Lie group X, with tangent space V at e, for every $v \in V$ there is a unique holomorphic homomorphism

$$\phi_v : \mathbf{C} \longrightarrow X$$

such that $d\phi_v$ takes the unit tangent vector to $\mathbf{C}$ at 0 to $v \in V$. (Cf. Hochschild, *Structure of Lie Groups*, p. 79 and p. 195). Moreover the function $\phi_v(t)$ in t *and* v is a holomorphic map $\mathbf{C} \times V \to X$. The *exponential map* $\exp: V \to X$ is defined by $\exp(v) = \phi_v(1)$. Because of the uniqueness property characterizing ϕ_v, $\phi_{sv}(t) = \phi_v(st)$, hence $\phi_v(t) = \exp(tv)$. Therefore, if we identify as usual the tangent space to V at 0 with V itself, the differential of exp at 0 is the identity map of V onto V. Returning to a compact connected X now, we first prove:

(1) *X is a commutative group.*

PROOF. In fact, for x in X, define C_x to be the conjugation map $X \to X, C_x(y) = xyx^{-1}$. The differential $(dC_x)_e$ is an automorphism of V and $x \longmapsto (dC_x)_e$ is a holomorphic map of X into $\mathrm{Aut}(V) \subset \mathrm{End}(V)$. Since $\mathrm{End}(V)$ is a finite-dimensional complex vector space and the only holomorphic functions on a compact connected complex manifold are constants, we deduce that $(dC_x)_e$ is independent of $x \in X$, hence $(dC_x)_e = (dC_e)_e = 1_V$. Now for any homomorphism $T: X_1 \to X_2$ of complex Lie groups,

$$T(\exp_{X_1} y) = \exp_{X_2}((dT)_e y).$$

This follows from the uniqueness property characterizing the homomorphisms $t \longmapsto \exp_{X_i}(tv)$ from $\mathbf{C}$ to X_i. It is easy to prove from this that

$$C_x(\exp y) = \exp((dC_x)_e y).$$

Since $(dC_x)_e = 1_V$, this shows that $C_x(\exp y) = \exp y$, so $\exp(V)$ is in the center of X. Since $d(\exp)$ is the identity, it follows from the implicit function theorem that exp defines a homeomorphism of a neighborhood of $0 \in V$ with a neighborhood of e in X. Since X is connected, this implies that $\exp(V)$ generates X as a group, and it follows that X is commutative.

(2) *The exponential map* exp: $V \to X$ *is a surjective homomorphism of complex Lie groups with kernel a lattice*† U *in* V, *and induces an isomorphism* $V/U \xrightarrow{\sim} X$, *i.e.* X *is a complex torus.*

Let $x, y \in V$. Since X is commutative, the map $\mathbf{C} \to X$ defined by $t \longmapsto (\exp tx).(\exp ty)$ is a holomorphic homomorphism, and the image of $\left(\frac{\partial}{\partial t}\right)_0$ by the tangent map is easily seen to be $x + y$. Now for any $z \in V$, the map $t \to \exp(tz)$ is characterized as the unique holomorphic homomorphism, whose tangent map takes $\left(\frac{\partial}{\partial t}\right)_0$ to $z \in V$. Hence $(\exp tx).(\exp ty) = \exp t(x + y)$ and putting $t = 1$, we find that exp is a homomorphism. It is surjective since on the one hand X is connected, while on the other hand $\exp(V)$ contains a neighborhood of e and hence an open and closed subgroup of X. The kernel U is a discrete subgroup of V, since there is a neighborhood N of 0 in V such that $\exp|_N : N \to X$ is injective. The induced homomorphism $V/U \to X$ is holomorphic by definition of structure of complex manifold on V/U, and is an algebraic isomorphism of groups. The tangent map at the identity of this map is an isomorphism, and hence by the inverse function theorem, the inverse is holomorphic at e and hence holomorphic everywhere on X (translations being holomorphic isomorphisms on both V/U and X). Therefore X is isomorphic to V/U. Since lattices are the only discrete subgroups of vector spaces with compact quotient, V must be a lattice.

†By definition, a *lattice* in a real vector space V is the subgroup generated by a basis of V.

From now on, we use additive notation for the group operation in X. We will fix the notation $\pi: V \to X$ for the exponential homomorphism for the rest of this chapter.

(3) *As an abstract group,* X *is divisible* (*i.e.* $nX = X$ *for* $n \in \mathbf{Z}$, $n \neq 0$) *and if for* $n \in \mathbf{Z}$, $n \neq 0$, X_n *is the subgroup of elements annihilated by* n, $X_n \simeq (\mathbf{Z}/n\mathbf{Z})^{2g}$.

PROOF. By (2), we see that as a real Lie group, X is isomorphic to $(\mathbf{R}/\mathbf{Z})^{2g} = (S^1)^{2g}$, where S^1 is the circle group. Hence we have (3).

(4) *We have canonical isomorphisms*

$$H^r(X, \mathbf{Z}) \simeq \left\{ \begin{array}{c} \text{group of alternating } r\text{-forms} \\ U \times \ldots \times U \longrightarrow \mathbf{Z} \end{array} \right\}.$$

PROOF. (V, π) is clearly the universal covering space of X, hence $U = \pi^{-1}(0)$ is exactly $\pi_1(X, 0)$. Since for any good topological space X

$$H^1(X, \mathbf{Z}) \simeq \mathrm{Hom}(\pi_1(X), \mathbf{Z}),$$

the assertion is correct for $r = 1$. Then to prove it for all r, it will suffice to show that cup product induces an isomorphism

$$\Lambda^r(H^1(X, \mathbf{Z})) \xrightarrow{\sim} H^r(X, \mathbf{Z}), \text{ all } r. \qquad (*)$$

But note that if (*) is correct for spaces X_1 and X_2 with finitely generated cohomologies, then by the Künneth formula, (*) holds for $X_1 \times X_2$:

$$\begin{array}{ccc} \Lambda^r(H^1(X_1 \times X_2, \mathbf{Z})) & \longrightarrow & H^r(X_1 \times X_2, \mathbf{Z}) \\ \| \wr & & \| \wr \\ \Lambda^r[H^1(X_1, \mathbf{Z}) \oplus H^1(X_2, \mathbf{Z})] & & \| \wr \\ \| \wr & & \\ \sum_{p+q=r} [\Lambda^p H^1(X_1, \mathbf{Z}) \otimes \Lambda^q H^1(X_2, \mathbf{Z}))] & \xrightarrow{\sim} & \sum_{p+q=r} H^p(X_1, \mathbf{Z}) \otimes H^q(X_2, \mathbf{Z}). \end{array}$$

(Note here that (*) for X_1, X_2 implies $H^r(X_i, \mathbf{Z})$ is torsion-free, hence the tor term in Künneth disappears.) But our torus X is a product of S^1's, for which (*) is trivially valid.

(5) *Computation of the groups $H^q(X, \Omega^p)$, where Ω^p = sheaf of holomorphic p-forms on X.*

The cohomology groups $H^q(X, \Omega^p)$ are one of the most significant invariants of any compact complex manifold X, and their computation for a torus will take up the rest of this section.

Let $V = T_{0,X}$ be the tangent space to X at 0 (regarded as a complex vector space), and let $T = \mathrm{Hom}_{\mathbf{C}}(V, \mathbf{C})$ be the complex cotangent space to X at 0. By translation with respect to the group law on X, every complex p-covector $\alpha \in \Lambda^p T$ extends to a translation invariant holomorphic p-form ω_α on X. In fact, let $T_x: X \to X$ be the map $T_x(y) = x+y$. Then define $(\omega_\alpha)_x = T^*_{-x}(\alpha)$. Moreover, the map $\alpha \longmapsto \omega_\alpha$ defines a homomorphism of sheaves:

$$\mathcal{O}_X \otimes_{\mathbf{C}} \Lambda^p T \longrightarrow \Omega^p \qquad (*)$$

which is easily checked to be an isomorphism. In other words, Ω^p is a *globally* free sheaf of $\mathcal{O}_X$-modules. Since the only global sections of $\mathcal{O}_X$ are constants, the global sections of Ω^p are exactly the translation-invariant p-forms ω_α. In fact, because of the isomorphism (*) we get:

$$H^q(X, \Omega^p) \cong H^q(X, \mathcal{O}_X \otimes \Lambda^p T) \cong H^q(X, \mathcal{O}_X) \otimes \Lambda^p T.$$

The main result that we want is

THEOREM. *If $\overline{T} = \mathrm{Hom}_{\mathbf{C}\text{-antilinear}}(V, \mathbf{C})$, then there are natural isomorphisms*

$$H^q(X, \mathcal{O}_X) \cong \Lambda^q \overline{T}$$

for all q, hence

$$H^q(X, \Omega^p) \cong \Lambda^p T \otimes \Lambda^q \overline{T}.$$

Our proof of this (due to C. P. Ramanujam and related to that of Weil [W2]) depends on the well-known Dolbeault resolution:

$$0 \longrightarrow \mathcal{O}_X \longrightarrow \mathscr{C}^{0,0} \xrightarrow{\overline{\partial}} \mathscr{C}^{0,1} \xrightarrow{\overline{\partial}} \mathscr{C}^{0,2} \longrightarrow \cdots$$

where $\mathscr{C}^{p,q}$ is the sheaf of C^∞ complex-valued differential forms of type-(p, q) on X, and $\overline{\partial}$ is the component of the exterior derivative d mapping $\mathscr{C}^{p,q}$ to $\mathscr{C}^{p,q+1}$. For background on this, see Gunning-Rossi, Ch. 6. The $\mathscr{C}^{p,q}$ are fine sheaves, hence the above resolution defines isomorphisms

$$H^q(X, \mathcal{O}_X) \cong \frac{\{\overline{\partial}\text{-closed } (0, q)\text{-forms on } X\}}{\overline{\partial}\{\text{space of } (0, q-1)\text{-forms on } X\}}.$$

Moreover, if $\mathscr{C} = \mathscr{C}^{0,0}$ is the sheaf of C^∞ complex-valued functions on X, then just as with holomorphic forms, there is an isomorphism

$$\phi_{p,q} : \mathscr{C} \otimes_{\mathbf{C}} [\Lambda^p T \otimes \Lambda^q \overline{T}] \xrightarrow{\approx} \mathscr{C}^{p,q}$$

taking $\Sigma f_i \otimes \alpha_i$ to $\Sigma f_i \omega_{\alpha i}$ where ω_α is the translation invariant (p, q)-form with value $\alpha \in \Lambda^p T \otimes \Lambda^q \overline{T}$ at 0. Note that these translation-invariant forms ω_α are all closed. In fact, since $\omega_{\alpha \wedge \beta} = \omega_\alpha \wedge \omega_\beta$, it is sufficient to check this for α of degree (1, 0) or (0, 1). Since $\pi: V \to X$ is a local isomorphism, it is sufficient to check that $d(\pi^*(\omega_\alpha)) = 0$. But considering α itself (which is in $T \oplus \overline{T}$) as a function on V, $\pi^*(\omega_\alpha) = d\alpha$. Therefore $d(\pi^*\omega_\alpha) = d^2\alpha = 0$.

Now let $\Lambda^\cdot = \bigoplus_q \Lambda^q \overline{T}$ be the exterior algebra on $\overline{T}$. Let $\mathfrak{a} = \Gamma(X, \mathscr{C})$. Then via $\phi_{0,q}$, we get an isomorphism

$$\mathfrak{a} \otimes_{\mathbf{C}} \Lambda^q \xrightarrow{\approx} \Gamma(X, \mathscr{C}^{0,q}).$$

If we define a differential $\overline{\partial}$ on the set of spaces on the left by $\overline{\partial}(f \otimes \alpha) = \overline{\partial} f \wedge \alpha$, then (because the ω_α are closed), the *complexes* $\mathfrak{a} \otimes_{\mathbf{C}} \Lambda^\cdot$ and $\Gamma(X, \mathscr{C}^{0,\cdot})$ are isomorphic. Therefore

$$H^q(X, \mathcal{O}_X) \cong H^q(\mathfrak{a} \otimes_{\mathbf{C}} \Lambda^\cdot).$$

Our aim is now to show that the inclusion $i: \Lambda^\cdot \to \mathfrak{a} \otimes_{\mathbf{C}} \Lambda^\cdot$ defines an isomorphism of cohomology, i.e. $\Lambda^q \xrightarrow{\sim} H^q(\mathfrak{a} \otimes_{\mathbf{C}} \Lambda^\cdot)$. We will do this by Fourier series. Let μ be the measure on X induced by the Euclidean measure on V, and so normalized that the volume $\mu(X)$ of X is 1. We define a $\mathbf{C}$-linear map $\mu: \mathfrak{a} \to \mathbf{C}$ by putting $\mu(f) = \int_X f\mu$. For any vector space W over $\mathbf{C}$, we denote by μ_W the

map $\mu\otimes 1_W$: $\mathfrak{a}\otimes W \to W$: in particular, we get a map μ_Λ: $\mathfrak{a}\otimes_{\mathbf{C}}\Lambda^\cdot \to \Lambda^\cdot$ which is $\Lambda^\cdot$-linear and such that $\mu_\Lambda \circ i = \mathrm{Id}_\Lambda$.

LEMMA 1. *For $\omega \in \mathfrak{a}\otimes_{\mathbf{C}}\Lambda^\cdot$, we have $\mu_\Lambda(\bar\partial\omega) = 0$.*

PROOF. Since μ_Λ is $\Lambda^\cdot$-linear, it suffices to prove that $\mu_\Lambda(\bar\partial f) = 0$ for $f \in \mathfrak{a}$. Choosing a basis $\omega_1, \dots, \omega_n$ of $\overline{T}$, we can expand $\bar\partial f \in \mathfrak{a}\otimes_{\mathbf{C}}\overline{T}$ as $\Sigma h_i \otimes \omega_i$. The coefficients h_i are all of the form $D(f)$, where D is some invariant vector field on X. Therefore the lemma follows from the elementary fact that if f is a C^∞-function on V, periodic with respect to the lattice U, and D is a translation-invariant vector field on V, then

$$\int_{V/U} D(f)\, dx = 0$$

(dx = some Euclidean volume element).

Let $U^* = \mathrm{Hom}(U, \mathbf{Z})$. If $\lambda \in U^*$, then λ extends to an $\mathbf{R}$-linear map λ: $V \to \mathbf{R}$ and we can then form the function $x \to e^{2\pi i\lambda(x)}$ on V. This function is invariant under the action of U, hence it equals $e_\lambda \circ \pi$, where e_λ is a C^∞-function on X. Now define a $\mathbf{C}$-linear map Q_λ: $\mathfrak{a} \to \mathbf{C}$ by $Q_\lambda(f) = \mu(e_{-\lambda}f) = \int_X e_{-\lambda}\cdot f\cdot\mu$. More generally, for any vector space W, define Q_λ: $\mathfrak{a}\otimes_{\mathbf{C}}W \to W$ by $Q_\lambda(f\otimes w) = \mu(e_{-\lambda}f).w$. The $Q_\lambda(f)$ are the Fourier coefficients of f: for every $f \in \mathfrak{a}\otimes_{\mathbf{C}}W$ we get the expansion

$$f = \sum_{\lambda\in U^*} e_\lambda \otimes Q_\lambda(f).$$

The Q_λ are compatible with $\mathbf{C}$-linear maps $W \to W'$ just as μ is in particular, Q_λ: $\mathfrak{a}\otimes_{\mathbf{C}}\Lambda^\cdot \to \Lambda^\cdot$ is a $\Lambda^\cdot$-linear map.

For the remainder of this proof, we choose a Hermitian norm $\|\ \|$ on the complex vector space V. As usual, this induces a norm on $\overline{T}$, hence on the whole exterior algebra $\Lambda^\cdot$.

Moreover, define the mapping $\overline{C}$: $U^* \to \overline{T}$ as follows:

$$U^* \longrightarrow \mathrm{Hom}_{\mathbf{R}}(V, \mathbf{R}) \subset \mathrm{Hom}_{\mathbf{R}}(V, \mathbf{C}) \cong [T \oplus \overline{T}] \xrightarrow[\text{projection}]{} \overline{T}.$$

This makes U^* into a lattice in $\overline{T}$, hence by restriction we get a norm $\|\ \|$ on U^* too.

LEMMA 2. (1) *The map $f \to \{Q_\lambda(f)\}_{\lambda\in U^*}$ is an isomorphism of $\mathfrak{a}$ onto the vector space of all maps Q: $U^* \to \mathbf{C}$ decreasing at ∞ faster than $\|\lambda\|^{-n}$, all n, i.e.*

$$|Q(\lambda)| = O(\|\lambda\|^{-n}),\ \textit{all } n.$$

(2) *For all $\omega \in \mathfrak{a}\otimes_{\mathbf{C}}\Lambda^p$*

$$Q_\lambda(\bar\partial\omega) = (-1)^p 2\pi i[Q_\lambda(\omega) \wedge \bar C(\lambda)].$$

PROOF. (1) is standard Fourier analysis. To prove (2), note that

$$\pi^*(\bar\partial e_{-\lambda}) = \bar\partial(e^{-2\pi i\lambda}) = -2\pi i e^{-2\pi i\lambda}.\bar\partial\lambda = \pi^*[-2\pi i e_{-\lambda}\otimes\bar C(\lambda)],$$

hence $\partial e_{-\lambda} = -2\pi i e_{-\lambda}\otimes\bar C(\lambda)$. Therefore, by Lemma 1, for all $\omega \in \mathfrak{a}\otimes\Lambda^p$,

$$\begin{aligned} 0 &= \mu_\Lambda(\bar\partial(\omega e_{-\lambda})) \\ &= \mu_\Lambda(e_{-\lambda}\cdot\bar\partial\omega) + (-1)^{p-1}\, 2\pi i\, \mu_\Lambda(\omega e_{-\lambda}\wedge\bar C(\lambda)) \\ &= Q_\lambda(\bar\partial\omega) + (-1)^{p-1}\, 2\pi i\, Q_\lambda(\omega)\wedge C(\lambda). \end{aligned}$$

The following is well known.

LEMMA 3. *Let W be a complex vector space, $D \in \mathrm{Hom}_{\mathbf{C}}(W, \mathbf{C})$. Then D extends to a map $D\lrcorner$: $\Lambda^p W \to \Lambda^{p-1}W$ for all p, called interior multiplication by D, such that*

(1)

$$D\lrcorner(X_1\wedge\dots\wedge X_p) = \sum_{k=1}^{p}(-1)^{p-k} D(X_k).X_1\wedge\dots\wedge\hat X_k\wedge\dots\wedge X_p;$$

(2) *in particular, if $DX_0 = 1$, for all $\omega \in \Lambda^\cdot W$,*

$$D\lrcorner(\omega\wedge X_0) + (D\lrcorner\omega)\wedge X_0 = \omega.$$

We are now all set to prove that i: $\Lambda^\cdot \to \mathfrak{a}\otimes_{\mathbf{C}}\Lambda^\cdot$ is a homotopy equivalence for $\bar\partial$-cohomology. For every $\lambda \in U^*$, $\lambda \neq 0$ define an element $\lambda^* \in \mathrm{Hom}_{\mathbf{C}}(\overline{T}, \mathbf{C})$ using the Hermitian inner product $\langle\ ,\ \rangle$ on $\overline{T}$:

$$\lambda^*(x) = \frac{\langle x, \overline{C}(\lambda)\rangle}{2\pi i\, \|\overline{C}(\lambda)\|^2}.$$

Then $2\pi i\ \lambda^*(\bar{C}(\lambda)) = 1$, and $\|\lambda^*\| \leqslant (2\pi)^{-1}.\|\lambda\|^{-1}$. For all $\omega \in \mathfrak{a} \otimes \Lambda^p$, we define $k(\omega) \in \mathfrak{a} \otimes \Lambda^{p-1}$ by means of its Fourier expansion as follows :

$$Q_\lambda(k(\omega)) = (-1)^{p-1}\lambda^* \lrcorner Q_\lambda(\omega), \text{ if } \lambda \neq 0$$

$$Q_0(k(\omega)) = 0.$$

It is easy to check by Lemma 2 and some easy estimates that one and only one such $k(\omega)$ exists. Then we assert:

$$\bar{\partial}k + k\bar{\partial} = 1_{a \otimes \Lambda} - i \circ \mu_\Lambda. \qquad (*)$$

In fact, for any $\omega \in \mathfrak{a} \otimes \Lambda^p$, we can check that both sides have the same Fourier coefficients. If $\lambda \neq 0$,

$$\begin{aligned} Q_\lambda(\bar{\partial}k\omega + k\bar{\partial}\omega) &= 2\pi i.\ Q_\lambda(k\omega) \wedge \bar{C}\lambda + \lambda^* \lrcorner Q_\lambda(\bar{\partial}\omega) \\ &= 2\pi i[(\lambda^* \lrcorner Q_\lambda\ \omega) \wedge \bar{C}\lambda + \lambda^* \lrcorner (Q_\lambda(\omega) \wedge \bar{C}\lambda)] \\ &= Q_\lambda(\omega) \end{aligned}$$

and $Q_\lambda(i(\mu_\Lambda\omega)) = 0$. If $\lambda = 0$, then $Q_0(k\bar{\partial}\omega) = 0$, and $Q_0(\bar{\partial}k\omega) = 0$, while $Q_0(\omega) = Q_0(i(\mu_\Lambda\omega))$. This proves (*).

It follows immediately from (*) that μ commutes with $\bar{\partial}$ and that $i \circ \mu$ is homotopic to the identity. Thus $i: \Lambda^\cdot \to \mathfrak{a} \otimes_{\mathbf{C}} \Lambda^\cdot$ induces isomorphisms in $\bar{\partial}$-cohomology as claimed.

REMARK 1. In the above isomorphism of $H^q(X, \mathcal{O}_X)$ with $\Lambda^q\bar{T}$, the cup product pairing

$$H^{q_1}(X, \mathcal{O}_X) \times H^{q_2}(X, \mathcal{O}_X) \longrightarrow H^{q_1+q_2}(X, \mathcal{O}_X)$$

corresponds to the exterior product

$$\Lambda^{q_1}\bar{T} \times \Lambda^{q_2}\bar{T} \longrightarrow \Lambda^{q_1+q_2}\bar{T}.$$

This follows from general sheaf theory, since we resolved the sheaf $\mathcal{O}_X$ of $\mathbf{C}$-algebras by a differential graded algebra $(\mathscr{C}^{0,q}, \bar{\partial})$. In such a case, cup product can be computed by multiplication in the resolving sheaf (Godement, §6.6).

COROLLARY 1. *The natural map induced by cup product*

$$\Lambda^q(H^1(X, \mathcal{O}_X)) \longrightarrow H^q(X, \mathcal{O}_X)$$

is an isomorphism.

REMARK 2. The same method used in the proof of the theorem enables one to compute the cohomology of the de Rham complex. Let $\mathscr{C}^n = \bigoplus_{p+q=n} \mathscr{C}^{p,q}$ be the sheaf of C^∞ complex-valued n-forms. Then

$$0 \longrightarrow \mathbf{C} \longrightarrow \mathscr{C}^0 \xrightarrow{d} \mathscr{C}^1 \xrightarrow{d} \cdots$$

is a fine resolution of the constant sheaf $\mathbf{C}$, hence as usual,

$$H^n(X, \mathbf{C}) \simeq \frac{\{d\text{-closed } n\text{-forms}\}}{d\{(n-1)\text{-forms}\}}.$$

Just as with $(0, q)$-forms, we obtain the result: for all d-closed n-forms ω, there is a unique translation-invariant n-form ω_α, $\alpha \in \Lambda^n \mathrm{Hom}_{\mathbf{R}}(V, \mathbf{C})$, such that

$$\omega - \omega_\alpha = d\eta, \text{ some } (n-1)\text{-form } \eta.$$

Therefore $H^n(X, \mathbf{C}) \simeq \Lambda^n[\mathrm{Hom}_{\mathbf{R}}(V, \mathbf{C})]$. Once again, these isomorphisms take cup product on the left hand side to exterior product on the right. Also, since

$$\mathrm{Hom}_{\mathbf{R}}(V, \mathbf{C}) \simeq T \oplus \bar{T},$$

this shows that

$$\begin{aligned} H^n(X, \mathbf{C}) &\simeq \Lambda^n(T \oplus \bar{T}) \\ &\simeq \bigoplus_{p+q=n} (\Lambda^p T \otimes \Lambda^q \bar{T}) \\ &\simeq \bigoplus_{p+q=n} H^q(X, \Omega^p). \end{aligned}$$

This is the famous Hodge decomposition.

REMARK 3. A closer look at what we have done so far reveals that the situation is a little complicated. Consider the three sheaves on X, embedded in one another as follows :

$$\mathbf{Z} \subset \mathbf{C} \subset \mathcal{O}_X$$

(**Z** and **C** being the constant sheaves). Looking at their H^1's, we have found three *independent evaluations* of these groups:

$H^1(X, \mathbf{Z}) \simeq \mathrm{Hom}(U, \mathbf{Z}) = U^*$, — via the isomorphism $H^1(Y, \mathbf{Z}) \simeq \mathrm{Hom}(\pi_1 Y, \mathbf{Z})$, all spaces Y.

first isom.

α

$H^1(X, \mathbf{C}) \simeq \mathrm{Hom}_{\mathbf{R}}(V, \mathbf{C}) = T' \oplus \overline{T}'$, — via the exact sequence

$$0 \longrightarrow \mathbf{C} \longrightarrow \mathscr{C}^0 \xrightarrow{d} \mathscr{C}^1_{\text{closed}} \longrightarrow 0$$

and $T' \oplus \overline{T}' \longrightarrow H^0(\mathscr{C}^1_{\text{closed}})$.

second isom.

β

$H^1(X, \mathscr{O}_X) \simeq \overline{T}'$, — via the exact sequence

$$0 \longrightarrow \mathscr{O}_X \longrightarrow \mathscr{C}^{0,0} \xrightarrow{\bar\partial} \mathscr{C}^{0,1}_{\bar\partial\text{-closed}} \longrightarrow 0$$

and $\overline{T}' \longrightarrow H^0(\mathscr{C}^{0,1}_{\bar\partial\text{-closed}})$.

third isom.

It is only natural to assume that the vertical arrows connecting the cohomology groups correspond, under these evaluations to the canonical maps (a) $\mathrm{Hom}(U, \mathbf{Z}) \to \mathrm{Hom}(U, \mathbf{Z}) \otimes_{\mathbf{Z}} \mathbf{C} \simeq \mathrm{Hom}_{\mathbf{R}}(V, \mathbf{C})$, and (b) projection of $T' \oplus \overline{T}'$ onto $\overline{T}'$. Let us check that this does occur.

POINT 1. The map $H^1(X, \mathbf{C}) \xrightarrow{\beta} H^1(X, \mathscr{O}_X)$. This can be computed by comparing the two resolutions. Let $C_{0,1}: \mathscr{C}^1 = \mathscr{C}^{1,0} \oplus \mathscr{C}^{0,1} \to \mathscr{C}^{0,1}$ be the projection. $C_{0,1}$ takes d-closed forms to $\bar\partial$-closed forms, hence we get a diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbf{C} & \longrightarrow & \mathscr{C}^0 & \xrightarrow{d} & \mathscr{C}^1_{d\text{-closed}} & \longrightarrow & 0 \\
 & & \downarrow & & \| & & \downarrow{\scriptstyle C_{0,1}} & & \\
0 & \longrightarrow & \mathscr{O}_X & \longrightarrow & \mathscr{C}^{0,0} & \longrightarrow & \mathscr{C}^{0,1}_{\bar\partial\text{-closed}} & \longrightarrow & 0.
\end{array}$$

This gives us a commutative diagram:

$$\begin{array}{ccccc}
T \oplus \overline{T} & \hookrightarrow & H^0(X, \mathscr{C}^1_{d\text{-closed}}) & \xrightarrow{\delta} & H^1(X, \mathbf{C}) \\
\downarrow{\scriptstyle \text{projection}} & & \downarrow{\scriptstyle C_{0,1}} & & \downarrow{\scriptstyle \beta} \\
\overline{T} & \hookrightarrow & H^0(X, \mathscr{C}^{0,1}_{\bar\partial\text{-closed}}) & \xrightarrow{\delta} & H^1(X, \mathscr{O}_X).
\end{array}$$

Thus β is the expected map.

COROLLARY 2. *β is surjective.*

POINT 2. The map $H^1(X, \mathbf{Z}) \xrightarrow{\alpha} H^1(X, \mathbf{C})$. Let $a \in H^1(X, \mathbf{Z})$. How does such an a determine a homomorphism $\tilde a$ from $\pi_1(X)$ to $\mathbf{Z}$? If $\phi: S^1 \to X$ is a loop in X corresponding to an element $[\phi] \in \pi_1(X)$, then $\tilde a([\phi])$ is found by considering $\phi^*(a) \in H^1(S^1, \mathbf{Z})$ and using the canonical isomorphism $\epsilon: H^1(S^1, \mathbf{Z}) \xrightarrow{\sim} \mathbf{Z}$:

$$\tilde a([\phi]) = \epsilon(\phi^*(a)).$$

In particular, for all $u \in U$, let $\phi_u: S^1 \to X$ be the loop

$$\phi_u(t) = \pi(tu) \text{ (where } S^1 \text{ is parametrized by } t \in \mathbf{R},$$

considered mod $\mathbf{Z}$).

Then a determines $\tilde a \in U^*$ by the rule

$$\tilde a(u) = \epsilon(\phi_u^*(a)).$$

Now suppose we push a into the sheaf **C**: we get $\alpha(a) \in H^1(X, \mathbf{C})$. According to our second evaluation, there is a unique $b \in T \oplus \overline{T}$ such that if ω_b is the invariant 1-form on X with value b at 0, then we get:

$$\begin{array}{ccc} H^0(X, \mathscr{C}^1_{\text{closed}}) & \xrightarrow{\delta} & H^1(X, \mathbf{C}) \\ \cup & & \cup \\ \omega_b & \longmapsto & \alpha(a). \end{array}$$

Pulling back to S^1, we find:

$$\begin{array}{ccc} H^0(S^1, \mathscr{C}^1_{\text{closed}}) & \xrightarrow{\delta} & H^1(S^1, \mathbf{C}) \\ \cup & & \cup \\ \phi_u^*(\omega_b) & \longrightarrow & \phi_u^*(\alpha(a)) \\ & & \| \\ & & \alpha(\phi_u^*(a)). \end{array}$$

But now it is an elementary matter to check that if η is a 1-form on S^1 (any such η is closed), if $\delta(\eta)$ is its image in $H^1(S^1, \mathbf{C})$ and if $\epsilon(\delta(\eta))$ is the image of $\delta(\eta)$ via the canonical isomorphism $\epsilon\colon H^1(S^1, \mathbf{C}) \xrightarrow{\sim} \mathbf{C}$, then

$$\epsilon(\delta(\eta)) = \int_{S^1} \eta.$$

Therefore

$$\begin{aligned} \tilde{a}(u) &= \epsilon(\phi_u^*(a)) \\ &= \epsilon(\delta(\phi_u^*(\omega_b))) \\ &= \int_{S^1} \phi_u^*(\omega_b) \\ &= \int_0^u \pi^*(\omega_b) \\ &= b(u). \end{aligned}$$

So $\tilde{a}$ is just the restriction of the function b on V to U.

Using compatibility of our evaluations with cup products, we have even proven now that we have the following compatibilities between the evaluations of the n^{th} cohomology groups:

$$\begin{array}{ccccc} H^n(X, \mathbf{Z}) & \underset{\text{first}}{\sim} & \Lambda^n(U^*) & & \\ \downarrow & & \downarrow & \Lambda^n \text{ of (inclusion } U^* \subset T \oplus \overline{T}) & \\ H^n(X, \mathbf{C}) & \underset{\text{second}}{\sim} & \Lambda^n(T \oplus \overline{T}) = \bigoplus_{p+q=n} \Lambda^p T \otimes \Lambda^q \overline{T} & & \\ \downarrow & & \downarrow & \text{projection onto } p=0,\ q=n \text{ factor} & \\ H^n(X, \mathscr{O}_X) & \underset{\text{third}}{\sim} & \Lambda^n(\overline{T}). & & \end{array}$$

2. Line bundles on a complex torus. We recall the well-known

THEOREM. *For all integers $p > 0$, $H^p(\mathbf{C}^N, \mathscr{O}) = (0)$.*

For a proof, cf. Gunning-Rossi, p. 28 and p. 184.

COROLLARY. $H^p(\mathbf{C}^N, \mathscr{O}^*) = (1)$, *all $p > 0$. In particular, all holomorphic line bundles on $\mathbf{C}^N$ are trivial.*

PROOF. Use the exact sequence

$$0 \longrightarrow \mathbf{Z} \longrightarrow \mathscr{O} \xrightarrow{e^{2\pi i(\ )}} \mathscr{O}^* \longrightarrow 0$$

and the fact that $H^p(\mathbf{C}^N, \mathbf{Z}) = (0)$, all $p > 0$.

We wish to give a direct geometric description of every (holomorphic) line bundle L on a complex torus X. By the corollary, the line bundle $\pi^*(L)$ on V is trivial. If we choose an isomorphism

$$\chi\colon \pi^*(L) \xrightarrow{\sim} \mathbf{C} \times V$$

the canonical action of U on $\pi^*(L)$ (i.e. the action such that the quotient of $\pi^*(L)$ by U is just the original bundle L) carries over by means of χ into a linear action of U on the trivial bundle covering the action of U on the base V by translations. Let us denote by H^* the multiplicative group $H^0(V, \mathscr{O}_V^*)$ of nowhere vanishing holomorphic functions on V. Since the only holomorphic automorphisms of a line bundle fixing the base are given by multiplication by non-vanishing holomorphic functions, we see that the action of U on $\mathbf{C} \times V$ is given by

$$(\alpha, z) \longmapsto \phi_u(\alpha, z) = (e_u(z).\alpha, z + u), \text{ all } u \in U \qquad \text{(A)}$$

where $e_u \in H^*$. Writing down the condition that

$\phi_u(\phi_{u'}(\alpha,z)) = \phi_{u+u'}(\alpha,z)$, we see that $u \longmapsto e_u$ is a 1-*cocycle* for U with coefficients in H^* :

$$e_{u+u'}(z) = e_u(z + u').e_{u'}(z).$$

Further, if the trivialization χ is altered by multiplication by a nowhere vanishing holomorphic function f on V, $\{e_u\}$ is replaced by the cohomologous cocycle :

$$e'_u(z) = e_u(z)\, f(z + u)\, f(z)^{-1}.$$

Therefore we have defined a map from $H^1(X, \mathcal{O}_X^*)$ to $H^1(U, H^*)$. But we can go in the other direction too. If we start with a 1-cocycle $\{e_u\}$ with coefficients in H^*, then define a line bundle L on X as the quotient of $\mathbf{C} \times V$ by the action of U given by $(\alpha,z) \longmapsto (e_u(z).\ \alpha,\ z+u)$. Therefore we have found an isomorphism

$$\phi : H^1(U, H^*) \xrightarrow{\approx} H^1(X, \mathcal{O}_X^*).$$

More generally, for any sheaf $\mathcal{F}$ on X, there is a natural map $\phi: H^1(U, \Gamma(U, \pi^*\mathcal{F})) \to H^1(X, \mathcal{F})$. The definition and properties of ϕ are recalled in an appendix to this section. Since $H^i(V, \mathcal{O}_V^*) = (1)$, all $i \geqslant 1$, the ϕ defined in the appendix is also an isomorphism. Let us check that the isomorphism just obtained and that of the appendix are the same. In fact, choose an open covering $\{V_i\}$ of X by small enough connected open sets V_i. Then

(a) $\pi^{-1}(V_i) =$ disjoint union of connected open sets $u + W_i$, all $u \in U$.

(b) If $\pi_i =$ restriction of π to W_i, $\pi_i : W_i \xrightarrow{\sim} V_i$ is a homeomorphism.

(c) If $V_i \cap V_j \neq \emptyset$, then $\exists\ u_{ij} \in V$ such that

$$\pi_j^{-1}(V_i \cap V_j) = \pi_i^{-1}(V_i \cap V_j) + u_{ij}.$$

The map ϕ of the appendix by definition takes a group 1-cocycle $\{e_u\}$ to the Čech 1-cocycle $\{f_{ij}\}$, $f_{ij} \in \Gamma(V_i \cap V_j, \mathcal{O}_X^*)$ defined by

$$f_{ij}(z) = e_{u_{ij}}(\pi_i^{-1}(z)).$$

But $\{f_{ij}\}$ defines the line bundle L which is the union of trivial line bundles $\mathbf{C} \times V_i$, modulo the patching

$$\begin{array}{ccc} \mathbf{C} \times V_i & & \mathbf{C} \times V_j \\ \cup & & \cup \\ \mathbf{C} \times (V_i \cap V_j) & \xrightarrow{\approx} & \mathbf{C} \times (V_i \cap V_j) \\ (\alpha, x) & \longmapsto & (\alpha\, f_{ij}(x), x). \end{array}$$

But π_i is an isomorphism of $\mathbf{C} \times W_i$ with $\mathbf{C} \times V_i$, so L can also be described as the union of trivial line bundles $\mathbf{C} \times W_i$, modulo the patching

$$\begin{array}{ccc} \mathbf{C} \times W_i & & \mathbf{C} \times W_j \\ \cup & & \cup \\ \mathbf{C} \times \pi_i^{-1}(V_i \cap V_j) & \xrightarrow{\approx} & \mathbf{C} \times \pi_j^{-1}(V_i \cap V_j) \\ (\alpha, x) & \longmapsto & (\alpha.f_{ij}(\pi_i(x)),\ x + u_{ij}) = \phi_{u_{ij}}(\alpha, x). \end{array}$$

Now the disjoint union of $\mathbf{C} \times W_i$ is just the line bundle $\mathbf{C} \times V$ pulled back to $\bigcup W_i$, and the set of above identifications is just the equivalence relation on this pull-back bundle induced by the equivalence relation on $\mathbf{C} \times V$ given by the action of the group U. Therefore, L is exactly $\mathbf{C} \times V$ modulo U.

On any complex analytic space X the exact sequence

$$0 \longrightarrow \mathbf{Z} \longrightarrow \mathcal{O}_X \xrightarrow{e^{2\pi i(\ )}} \mathcal{O}_X^* \longrightarrow 0$$

† According to the conventions of the appendix, we should take the action of U on H^* as given by $(u\,h)\,(z) = h(z - u)$, $u \in U$, $z \in V$. But then, if e_u satisfies the condition above, $f_u = e_{-u}$ is a 1-cocycle for this action, and conversely. Thus, such associated 1- cocycle is given by $f_{ij} \in \Gamma(V_i \cap V_j,\ \mathcal{O}_X^*)$,

$$f_{ij}(z) = f_{-u_{ij}}(\pi_i^{-1}(z)) = e_{u_{ij}}(\pi_i^{-1}(z)),$$

which is the formula we have above.

defines a co-boundary $\delta: H^1(X, \mathcal{O}_X^*) \to H^2(X, \mathbf{Z})$. If a line bundle L corresponds to a cohomology class $\lambda \in H^1(X, \mathcal{O}_X^*)$, then $\delta(\lambda)$ is called the *first Chern class* of L. In our case, suppose L is defined as above by a 1-cocycle $\{e_u\}$ with values in H^*. We want to calculate the first Chern class of the corresponding line bundle. First notice that since $H^i(V, \mathbf{Z}) = (0)$ for $i > 0$, it follows from the appendix that the maps ϕ: $H^i(U, \mathbf{Z}) = H^i(U, H^0(V, \mathbf{Z})) \to H^i(X, \mathbf{Z})$ are isomorphisms. If H is the ring of holomorphic functions on V, we have an exact sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^0(V, \pi^*(\mathbf{Z})) & \longrightarrow & H^0(V, \pi^*(\mathcal{O}_X)) & \xrightarrow{e^{2\pi i(\ )}} & H^0(V, \pi^*(\mathcal{O}_X^*)) & \longrightarrow & 0 \\ & & \| & & \| & & \| & & \\ & & \mathbf{Z} & & H & & H^* & & \end{array}$$

(since V is simply connected), so that by the compatibility of ϕ with δ (see Appendix) we get the diagram

$$\begin{array}{ccc} H^1(U, H^*) & \xrightarrow{\delta} & H^2(U, \mathbf{Z}) \\ \wr\downarrow & & \wr\downarrow \\ H^1(X, \mathcal{O}_X^*) & \xrightarrow{\delta} & H^2(X, \mathbf{Z}). \end{array}$$

Hence identifying $H^2(U, \mathbf{Z})$ and $H^2(X, \mathbf{Z})$ by the above homomorphism, the Chern class of L is simply $\delta(\mathrm{cl}\,\{e_u\})$. Write $e_u(z) = e^{2\pi i f_u(z)}$ with f_u holomorphic in V. Then by definition, $\delta(\mathrm{cl}\,\{e_u\}) \in H^2(U, \mathbf{Z})$ is given by the 2-cocycle $F(u_1, u_2)$ on U with coefficients in $\mathbf{Z}$ given by

$$F(u_1, u_2) = f_{u_2}(z + u_1) - f_{u_1+u_2}(z) + f_{u_1}(z) \in \mathbf{Z}. \qquad (*)$$

Now we use the following standard fact.

LEMMA. *The map which associates to any map $F: U \times U \to \mathbf{Z}$ the map $AF: U \times U \to \mathbf{Z}$ defined by $AF(u_1, u_2) = F(u_1, u_2) - F(u_2, u_1)$ maps the group of 2-cocycles $Z^2(U, \mathbf{Z})$ into the space of alternating linear maps $U \times U \to \mathbf{Z}$, and induces an isomorphism*

$$A: H^2(U, \mathbf{Z}) \xrightarrow{\sim} \mathrm{Hom}\,(\Lambda^2 U, \mathbf{Z}) \cong \Lambda^2\,\mathrm{Hom}\,(U, \mathbf{Z}).$$

Further, for $\xi, \eta \in \mathrm{Hom}(U, \mathbf{Z}) = H^1(U, \mathbf{Z})$, we have $A(\xi \cup \eta) = \xi \wedge \eta$.

PROOF. First we check that if $F \in Z^2(U, \mathbf{Z})$, $E = AF$ is bilinear. We have

$$F(u_2, u_3) - F(u_1 + u_2, u_3) + F(u_1, u_2 + u_3) - F(u_1, u_2) = 0,\ u_i \in U. \qquad (i)$$

In this equation, instead of u_1, u_2 and u_3, substitute u_3, u_1 and u_2 (respectively u_1, u_3 and u_2) and call the equation so obtained (ii) (resp. (iii)). Then (i) + (ii) − (iii) gives us that

$$E(u_3, u_1 + u_2) = E(u_3, u_1) + E(u_3, u_2).$$

Since $E(u, u) = 0$ and $E(u, v) = -E(v, u)$, it follows that E is alternating bilinear. Now suppose $F = \delta G$ is a coboundary. Then

$$\begin{aligned} AF(u_1, u_2) &= (\delta G)(u_1, u_2) - (\delta G)(u_2, u_1) \\ &= [G(u_2) - G(u_1 + u_2) + G(u_1)] - \\ &\quad - [G(u_1) - G(u_1 + u_2) + G(u_2)] = 0. \end{aligned}$$

Hence A induces a homomorphism $H^2(U, \mathbf{Z}) \to \mathrm{Hom}(\Lambda^2 U, \mathbf{Z}) \cong \Lambda^2\mathrm{Hom}(U, \mathbf{Z})$.

Now, since we have an isomorphism ϕ of $H^*(U, \mathbf{Z})$ onto $H^*(X, \mathbf{Z})$ where X is a torus, taking cup products to cup products (see Appendix), and we know that $H^*(X, \mathbf{Z})$ is the exterior algebra on $H^1(X, \mathbf{Z})$, it follows that $H^*(U, \mathbf{Z})$ is also the exterior algebra on $H^1(U, \mathbf{Z}) = \mathrm{Hom}(U, \mathbf{Z})$. Thus, to prove that A is an isomorphism, it suffices to prove the last statement of the lemma. But now, if ξ(resp. η) is given by the homomorphism f(resp. g) of U into $\mathbf{Z}$, $\xi \cup \eta$ is given by the 2-cocycle (see Appendix) $c(s, t) = f(s).g(t)$, so that $A(\xi \cup \eta)$ is given by the map: $A(\xi \cup \eta)(s, t) = f(s)g(t) - f(t)g(s) = (f \wedge g)(s, t)$.

REMARK. We have thus an isomorphism $H^2(X, \mathbf{Z}) \xleftarrow{\sim} H^2(U, \mathbf{Z}) \xrightarrow{A} \Lambda^2\mathrm{Hom}(U, \mathbf{Z})$. This coincides with the isomorphism $H^2(X, \mathbf{Z}) \to \Lambda^2\mathrm{Hom}(U, \mathbf{Z})$ defined in §1, using cup product in $H^*(X, \mathbf{Z})$ and the isomorphism $H^1(X, \mathbf{Z}) \xrightarrow{\approx} \mathrm{Hom}(U, \mathbf{Z})$. In fact, ϕ commutes with cup products and A has the property that it maps cup product into exterior product, by the lemma, and

ϕ: $H^1(U, \mathbf{Z}) = \mathrm{Hom}(U, \mathbf{Z}) \to H^1(X, \mathbf{Z})$ is easily checked to coincide with the inverse of the isomorphism of §1 using the naturality of ϕ. Thus, in future, we can unambiguously identify $H^i(X, \mathbf{Z})$ with $\Lambda^i \mathrm{Hom}(U, \mathbf{Z})$.

Returning to the line bundle L arising from an $\{e_u\} \in Z^1(U, H^*)$ we state formally our conclusions as a

PROPOSITION. *The Chern class of the line bundle corresponding to $\{e_u\} \in Z^1(U, H^*)$ is the alternating 2-form on U with values in $\mathbf{Z}$ given by*

$$E(u_1, u_2) = f_{u_2}(z + u_1) + f_{u_1}(z) - f_{u_1}(z + u_2) - f_{u_2}(z), \quad (z \text{ arbitrary in } V) \tag{**}$$

where

$$e_u(z) = e^{2\pi i f_u(z)}.$$

COROLLARY. *If we extend E $\mathbf{R}$-linearly to a map $V \times V \to \mathbf{R}$, E satisfies the identity $E(ix, iy) = E(x, y)$ for $x, y \in V$.*

PROOF. In fact, since E represents an element of $H^2(X, \mathbf{Z})$ in the image of $H^1(X, \mathcal{O}_X^*) \to H^2(X, \mathbf{Z})$, its image by $H^2(X, \mathbf{Z}) \to H^2(X, \mathcal{O}_X)$ must be zero (and conversely). Now, this last map factorises as $H^2(X, \mathbf{Z}) \xrightarrow{i} H^2(X, \mathbf{C}) \xrightarrow{j} H^2(X, \mathcal{O}_X)$. If we put $\mathrm{Hom}_{\mathbf{R}}(V, \mathbf{C}) = \mathrm{Hom}_{\mathbf{C}}(V, \mathbf{C}) \oplus \mathrm{Hom}_{\mathbf{C}\text{-anti}}(V, \mathbf{C}) = T \oplus \overline{T}$, we have established isomorphisms $H^2(X, \mathbf{C}) \simeq \Lambda^2(T \oplus \overline{T}) \simeq (\Lambda^2 T) \oplus (T \otimes \overline{T}) \oplus (\Lambda^2 \overline{T})$, and $H^2(X, \mathcal{O}_X) \simeq \Lambda^2 \overline{T}$, and j goes over into the projection $\Lambda^2(T \oplus \overline{T}) \to \Lambda^2 \overline{T}$. Further, $i(E)$ is nothing but the real linear extension of E (cf. Remark 3, §1), which again we denote by E. Write $E = E_1 + E_2 + E_3$, where $E_1 \in \Lambda^2 T$, $E_2 \in \Lambda^2 \overline{T}$, and $E_3 \in T \otimes \overline{T}$. The reality of E implies that $E_1 = \overline{E}_2$, so that $j(E) = 0$ if and only if $E = E_3$, and this holds if and only if $E(x, y) = E(ix, iy)$.

Our next aim is to give as explicitly as possible all line bundles on the complex torus X, or equivalently, to find the simplest kind of representing cocycles $\{e_u\}$ for all cohomology classes in $H^1(U, H^*)$. This is in turn equivalent to finding a system of functions $\{f_u\}_{u \in U}$ holomorphic in V and satisfying (*).

Thus we *assume* given to us an alternating form $E: U \times U \to \mathbf{Z}$, with $E(ix, iy) = E(x, y)$ and we seek to find $\{f_u\}$ satisfying (*) and (**). Let us look for solutions f_u which are linear in z (not necessarily vanishing at 0).

We use the following elementary result.

LEMMA. *Let V be a complex vector space. There is a 1-1 correspondence between the Hermitian forms H on V and the real skew-symmetric forms E on V satisfying the identity $E(ix, iy) = E(x, y)$, which is given by*

$$E(x, y) = \mathrm{Im}\ H(x, y)$$

$$H(x, y) = E(ix, y) + i\,E(x, y).$$

The proof is left to the reader.

Let H correspond to the given E; then one checks immediately that the functions

$$f_u(z) = \frac{1}{2i} H(z, u) + \beta_u$$

satisfy (**) for any constants β_u, and the reader can also check if he likes that these are the only linear solutions of (**), holomorphic in z modulo coboundaries. Substituting in (*), we get a further condition:

$$\tfrac{1}{2}H(u_1, u_2) + i\beta_{u_1} + i\beta_{u_2} - i\beta_{u_1+u_2} \in i\mathbf{Z}$$

for all $u_1, u_2 \in U$. Writing $i\beta_u = \gamma_u + \frac{1}{4}H(u, u)$, this reduces to

$$\gamma_{u_1} + \gamma_{u_2} - \gamma_{u_1+u_2} + \tfrac{1}{2}\, iE(u_1, u_2) \in i\mathbf{Z}.$$

Now it is still permissible to modify if_u by the coboundary of a $\mathbf{C}$-linear form L on V, or what is the same, we may replace γ_u by $\gamma_u - L(u)$ with $L: V \to \mathbf{C}$ being $\mathbf{C}$-linear. The above equation shows that $\mathrm{Re}\gamma_u$ is additive in U, and hence extends to an $\mathbf{R}$-linear map $\lambda: V \to \mathbf{R}$, and there is a unique $\mathbf{C}$-linear form L on V with $\mathrm{Re}L = \lambda$ (viz., the form defined by $L(v) = \lambda(v) - i\lambda(iv)$). Modifying γ by this L, we may assume that γ is pure imaginary. Writing $\alpha(u) = e^{2\pi\gamma_u}$ we see that α has to satisfy the conditions

$$|\alpha(u)| = 1$$

$$\frac{\alpha(u_1+u_2)}{\alpha(u_1)\alpha(u_2)} = e^{i\pi E(u_1,u_2)}.$$

We can check that given E, there always exists such an α, or equivalently, that there always exists a map $\delta\colon U \to \mathbf{R}$ such that

$$\delta(u_1+u_2) - \delta(u_1) - \delta(u_2) \equiv \tfrac{1}{2}E(u_1,u_2) \pmod 1 \text{ for all } u_1, u_2 \in U.$$

This is left as an exercise to the reader.

We have thus proved the

LEMMA. *Let H be a hermitian form on V such that if $E = \operatorname{Im} H$, $E(U\times U) \subset \mathbf{Z}$. Let $\alpha\colon U \to \mathbf{C}_1^* = \{z \in \mathbf{C}^* \mid |z| = 1\}$ be a map with*

$$\alpha(u_1+u_2) = e^{i\pi E(u_1,u_2)}.\alpha(u_1)\alpha(u_2),\ u_i \in U.$$

Such maps α exist for any given H as above. If we put

$$e_u(z) = \alpha(u)\, e^{\pi H(z,u)+\frac{1}{2}\pi H(u,u)}$$

then $u \longmapsto e_u$ is a 1-cocycle on U with coefficients in $H^0(V, \mathcal{O}_V^*) = H^*$, the Chern class of the associated line bundle being $E \in H^2(X, \mathbf{Z})$.

DEFINITION. *$L(H,\alpha)$ is the quotient of $\mathbf{C}\times V$ for the action of U given by $\phi_u(\lambda, z) = (\alpha(u).e^{\pi H(z,u)+\frac{1}{2}\pi H(u,u)}.\ \lambda,\ z+u)$.*

Note that the map $(H, \alpha) \longmapsto \{e_u\}$ satisfies the condition that if $\{e_u^{(i)}\}$ corresponds to (H_i, α_i), $\{e_u^{(1)}.e_u^{(2)}\}$ corresponds to $(H_1+H_2, \alpha_1.\alpha_2)$. Therefore we have an isomorphism of line bundles

$$L(H_1, \alpha_1) \otimes L(H_2, \alpha_2) \simeq L(H_1+H_2, \alpha_1\alpha_2).$$

The main theorem of this section is

THEOREM OF APPELL-HUMBERT. *Any line bundle L on the complex torus X is isomorphic to an $L(H,\alpha)$ for a uniquely determined (H,α) satisfying the conditions of the above lemma. We have isomorphic exact sequences*

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \operatorname{Hom}(U, \mathbf{C}_1^*) & \longrightarrow & \{\text{Group of data } (H,\alpha)\} & \longrightarrow & \left\{\begin{array}{l}\text{Group of hermitian}\\ H: V\times V \longrightarrow \mathbf{C} \text{ with}\\ (\operatorname{Im} H)(U\times U)\subset \mathbf{Z}\end{array}\right\} & \longrightarrow & 0\\
 & & \wr\downarrow \lambda & & \wr\downarrow \mu & & \wr\downarrow \nu & & \\
0 & \longrightarrow & \operatorname{Pic}^0 X & \longrightarrow & \operatorname{Pic} X & \xrightarrow{C'} & \operatorname{Ker}[H^2(X,\mathbf{Z}) \longrightarrow H^2(X,\mathcal{O}_X)] & \longrightarrow & 0
\end{array}$$

where $\operatorname{Pic} X$ *is the group of line bundles on* X, $\operatorname{Pic}^0 X$ *the subgroup of those which are topologically trivial and the last vertical map is given by* $H \longmapsto \operatorname{Im} H$ *(with the usual identification of* $H^2(X,\mathbf{Z})$ *with alternating integral 2-forms on* U*).*

PROOF. We have already shown that an alternating integral 2-form E on U, considered as an element in $H^2(X,\mathbf{Z})$, maps into 0 in $H^2(X,\mathcal{O}_X)$ if and only if $E(ix,iy) = E(x,y)$ when E is extended $\mathbf{R}$-linearly to $V\times V$; that is, if and only if it is $\operatorname{Im} H$ for H Hermitian. Thus ν is an isomorphism. By definitions and the above lemma stating existence of α for given H, the first row is exact. Since the topological triviality of a line bundle L is equivalent to the vanishing of its Chern class, and since ν is an isomorphism, the second row is also exact.

To prove the theorem, it suffices to show that λ is an isomorphism. If $\alpha \in \operatorname{Hom}(U, \mathbf{C}_1^*)$ with $\lambda(\alpha) = 1$, we can find $g \in H^* = H^0(V, \mathcal{O}_V^*)$ with

$$\frac{g(z+u)}{g(z)} = \alpha(u).$$

If K is a compact set in V with $K+U = V$, it follows that for any $z \in V$, $|g(z)| \leqslant \operatorname{Sup}_K |g(z)|$, since $|\alpha| = 1$. Hence g can only be a constant, so $\alpha = 1$, which shows that λ is injective. Consider the commutative diagram

$$\begin{array}{ccccc}
H^1(U,\mathbf{C}) & \longrightarrow & H^1(U,H) & \xrightarrow{e^{2\pi i(\ )}} & \operatorname{Ker}[H^1(U,H^*) \longrightarrow H^2(U,\mathbf{Z})]\\
\wr\downarrow & & \wr\downarrow & & \wr\downarrow\\
H^1(X,\mathbf{C}) & \longrightarrow & H^1(X,\mathcal{O}_X) & \xrightarrow{e^{2\pi i(\ )}} & \operatorname{Ker}[H^1(X,\mathcal{O}_X^*) \longrightarrow H^2(X,\mathbf{Z})] = \operatorname{Pic}^0 X
\end{array}$$

where the vertical maps are isomorphisms and the maps denoted by $e^{2\pi i(\ )}$ are surjective. But we proved in §1 that $H^1(X,\mathbf{C}) \to H^1(X,\mathcal{O}_X)$ is surjective. It follows therefore that every line bundle $L \in \operatorname{Pic}^0(X)$ is presentable in the form $\mathbf{C}\times V$ modulo an action of U of form $\phi_u(\lambda, z) = (\lambda.\alpha(u),\ z+u)$, where $\alpha\colon U \to \mathbf{C}^*$ is a homomorphism.

But as we saw on p. 20, by an automorphism of $\mathbf{C} \times V$, we can always normalize such actions so that $\text{Image}(\alpha) \subset \mathbf{C}_1^*$. Therefore λ is surjective.

APPENDIX TO §2

We want to study cohomology of sheaves in the situation: $Y = X/G$, where G is a discrete group, acting freely and discontinuously on a good topological space X (i.e. $\forall\, x \in X$, x has a neighborhood U_x such that $U_x \cap \sigma(U_x) = \emptyset$, all $\sigma \in G, \sigma \neq e$).

Let $\pi: X \to Y$ be the projection.

First recall the definitions of the cohomology of abstract groups.

Let M be a G-module and let

$C^p(G, M) = \{\text{group of functions } f: G^p \longrightarrow M\}$;

$\delta: C^p \longrightarrow C^{p+1}$ the map

$$\delta f(\sigma_0, \dots, \sigma_p) = \sigma_0(f(\sigma_1, \dots, \sigma_p)) + \sum_{i=0}^{p-1} (-1)^{i+1} f(\sigma_0, \dots, \sigma_i \cdot \sigma_{i+1}, \dots, \sigma_p) + (-1)^{p+1} f(\sigma_0, \dots, \sigma_{p-1});$$

$Z^p(G, M) = \text{Ker}(\delta)$; $B^p(G, M) = \text{Im}(\delta)$;

$H^p(G, M) = Z^p(G, M)/B^p(G, M)$

$= \text{derived functors of } M \longmapsto H^0(G, M), \text{ where}$

$H^0(G, M) = \{m \in M \mid \sigma(m) = m, \text{ all } \sigma \in G\}$ (also written M^G).

Given a G-linear pairing $M \times N \xrightarrow{*} P$ of G-modules, get

$$\cup : H^p(G, M) \times H^q(G, N) \longrightarrow H^{p+q}(G, P) \text{ via}$$

$$f \cup g(\sigma_1, \dots, \sigma_{p+q}) = f(\sigma_1, \dots, \sigma_p) * (\sigma_1 \cdot \dots \cdot \sigma_p) g(\sigma_{p+1}, \dots, \sigma_{p+q}),$$

all $f \in C^p(G, M)$, $g \in C^q(G, N)$.

We want the result:

$\forall$ sheaves $\mathscr{F}$ on Y, there is a natural map

$$\phi: H^p(G, \Gamma(X, \pi^*\mathscr{F})) \longrightarrow H^p(Y, \mathscr{F}).$$

It has the properties:

(a) If

$$0 \longrightarrow \mathscr{F}' \longrightarrow \mathscr{F} \longrightarrow \mathscr{F}'' \longrightarrow 0$$

is an exact sequence of sheaves on Y, and

$$0 \longrightarrow \Gamma(X, \pi^*\mathscr{F}') \longrightarrow \Gamma(X, \pi^*\mathscr{F}) \longrightarrow \Gamma(X, \pi^*\mathscr{F}'') \longrightarrow 0$$

is exact, then we get a homomorphism from the cohomology sequence of $H^p(G, \cdot)$ to that of $H^p(Y, \cdot)$.

(b) The natural maps ϕ are compatible with cup product.

(c) If

$$H^i(X, \pi^*\mathscr{F}) = (0), \quad i \geqslant 1,$$

then

$$\phi: H^p(G, \Gamma(X, \pi^*\mathscr{F})) \longrightarrow H^p(Y, \mathscr{F})$$

is an isomorphism.

To define ϕ, choose a covering $\{V_i\}_{i \in I}$ of Y such that for each i,

(1) $\pi^{-1}(V_i) = \bigcup_{\sigma \in G} \sigma(U_i)$, $U_i \subset X$ open such that res $\pi: U_i \xrightarrow{\sim} V_i$,

(2) $\forall\, i, j$, there exists at most one $\sigma \in G$ such that $U_i \cap \sigma U_j \neq \emptyset$; call it σ_{ij} if it exists.

Define a map from group co-chains to Čech co-chains:

$$\phi_p : C^p(G, \Gamma(\pi^*\mathscr{F})) \longrightarrow C^p(\{V_i\}, \mathscr{F})$$

by

$$(\phi_p f)_{i_0, \dots, i_p} = \text{res} \circ (\pi^*)_{i_0}^{-1}[f(\sigma_{i_0, i_1}, \dots, \sigma_{i_{p-1}, i_p})]$$

where $(\pi^*)_i^{-1}: \Gamma(X, \pi^*\mathscr{F}) \longrightarrow \Gamma(V_i, \mathscr{F})$ is the map

$$\Gamma(X, \pi^*\mathscr{F}) \xrightarrow{\text{res}} \Gamma(U_i, \pi^*\mathscr{F}) \xleftarrow[\pi^*]{\approx} \Gamma(V_i, \mathscr{F}).$$

It is easy to check that $\delta\phi_p = \phi_{p+1}\delta$, hence the ϕ_p induce a map $\phi: H^p(G, \Gamma(X, \pi^*\mathscr{F})) \to H^p(Y, \mathscr{F})$. Properties (a) and (b) follow immediately by computation. To prove (c), we use induction on p: for $p = 0$, it is obvious. In general, embed $\mathscr{F}$ in an injective $\mathscr{O}_Y$-sheaf $\mathscr{F}'$ and let $\mathscr{F}'' = \mathscr{F}'/\mathscr{F}$. Then we find

$$0 \longrightarrow \Gamma(X, \pi^*\mathscr{F}) \longrightarrow \Gamma(X, \pi^*\mathscr{F}') \longrightarrow \Gamma(X, \pi^*\mathscr{F}'') \longrightarrow H^1(X, \pi^*\mathscr{F}) = (0)$$

hence

$$\begin{array}{ccccccc} H^{p-1}(G, \Gamma(\pi^*\mathscr{F}')) & \longrightarrow & H^{p-1}(G, \Gamma(\pi^*\mathscr{F}'')) & \longrightarrow & H^p(G, \Gamma(\pi^*\mathscr{F})) & \longrightarrow & H^p(G, \Gamma(\pi^*\mathscr{F}')) \\ \downarrow \phi_1 & & \downarrow \phi_2 & & \downarrow \phi_3 & & \downarrow \\ H^{p-1}(Y, \mathscr{F}') & \longrightarrow & H^{p-1}(Y, \mathscr{F}'') & \longrightarrow & H^p(Y, \mathscr{F}) & \longrightarrow & H^p(Y, \mathscr{F}'). \end{array}$$

It suffices to prove that $\Gamma(\pi^*\mathscr{F}')$ is an injective G-module, and that $H^i(X, \pi^*\mathscr{F}') = (0)$, $i \geqslant 1$, because then it follows that $H^i(X, \pi^*\mathscr{F}'') = (0)$, $i \geqslant 1$, hence ϕ_1, ϕ_2 are isomorphisms by the induction hypothesis, hence ϕ_3 is an isomorphism. We need

LEMMA. *If $\mathscr{F}$ is an injective $\mathscr{O}_Y$-sheaf, then $\pi^*\mathscr{F}$ is a flasque $\mathscr{O}_X$-sheaf and $\Gamma(\pi^*\mathscr{F})$ an injective G-module.*

PROOF. For all G-modules M, let M be the constant sheaf on X with value M. There is an obvious action of G on M compatible with its action on X. Then G acts also on $\pi_*(M)$, so we can form $\pi_*(M)^G$. It is easy to check that

$$\mathrm{Hom}_G(M, \Gamma(\pi^*\mathscr{F})) \simeq \mathrm{Hom}_{\mathscr{O}_Y}(\pi_*(M)^G, \mathscr{F}).$$

So if $M_1 \subset M_2$, then $\pi_*(M_1)^G \subset \pi_*(M_2)^G$, hence

$$\mathrm{Hom}_{\mathscr{O}_Y}(\pi_*(M_2)^G, \mathscr{F}) \to \mathrm{Hom}_{\mathscr{O}_Y}(\pi_*(M_1)^G, \mathscr{F})$$

is surjective, hence $\mathrm{Hom}_G(M_2, \Gamma(\pi^*\mathscr{F})) \to \mathrm{Hom}_G(M_1, \Gamma(\pi^*\mathscr{F}))$ is surjective. This shows that $\Gamma(\pi^*\mathscr{F})$ is injective. Secondly, $\mathscr{F}$ injective implies $\mathscr{F}$ flasque, and since π is a local homeomorphism, then $\pi^*\mathscr{F}$ is flasque too. (Cf. Grothendieck, *Sur quelques points d'algèbre homologique*, Tôhoku Math. J. (1957), esp. Ch. V, p. 195.)

3. Algebraizability of tori. We have seen that any line bundle L on the complex torus $X = V/U$ is isomorphic to a unique line bundle of the form $L(H, \alpha)$ where $H: V \times V \to \mathbf{C}$ is hermitian with $E = \mathrm{Im}\, H$ integral on $U \times U$, and α is a map $U \to \mathbf{C}_1^*$, satisfying $\alpha(u_1 + u_2) = e^{i\pi E(u_1, u_2)}\alpha(u_1).\alpha(u_2)$. $L(H, \alpha)$ is the quotient of $\mathbf{C} \times V$ for the action of U given by

$$\phi_u(\lambda, z) = (e_u(z).\lambda, z + u)$$
$$e_u(z) = \alpha(u)\, e^{\pi H(z,u) + \frac{1}{2}\pi H(u,u)}.$$

We now investigate the sections of $L(H, \alpha)$. These sections are in a natural one-one correspondence with sections θ of the trivial bundle $\mathbf{C} \times V$ over V (i.e. holomorphic functions θ on V) which are invariant under the above action of U, that is, which satisfy the functional equation

$$\theta(z + u) = e_u(z)\,\theta(z) = \alpha(u).\, e^{\pi H(z,u) + \frac{1}{2}\pi H(u,u)}\,\theta(z),\ z \in V,\ u \in U.$$

Such a function is called a *theta-function* for the hermitian form H and the multiplicator α.

First consider the case when H is degenerate. Since $E = \mathrm{Im}\, H$ and $H(x, y) = E(ix, y) + iE(x, y)$, we have

$$N = \{x \in V \mid H(x, y) = 0,\ \forall\, y \in V\} = \{x \in V \mid E(x, y) = 0,\ \forall\, y \in V\}.$$

It follows from the first expression for N that N is a complex subspace of V. And since E is integral on $U \times U$, it follows from the second expression for N that $N \cap U$ is a lattice in N. If θ is an associated theta-function, we must have

$$\theta(z + u) = \alpha(u)\,\theta(z),\ \forall\, u \in N \cap U.$$

Thus, if K is a compact subset of N with $N = K + (N \cap U)$, we must have

$$|\,\theta(z_0 + z')\,| \leqslant \sup_{\zeta \in K} |\,\theta(z_0 + \zeta)\,| = c(z_0),$$

for all $z' \in N$. Therefore, by the maximum principle for holomorphic functions, $\theta(z_0 + z') = \theta(z_0)$ for $z' \in N$ and θ is constant on cosets mod N. It follows from the earlier equality that if $\theta \neq 0$, then $\alpha(u) = 1$ for $u \in N \cap U$. Thus, if η: $V \to V/N$ is the natural map, we see that any theta-function for (H, α) is of the form $\bar{\theta} \circ \eta$, where $\bar{\theta}$ is a theta-function on V/N for the lattice $\eta(U)$, the hermitian form $\bar{H}$ induced by H, and the multiplicator $\bar{\alpha}$ obtained from α by passage to quotient from U to $U/N \cap U$. Now $\bar{H}$ is non-degenerate on $\bar{V} = V/N$. Thus the study of the theta-functions for (H, α) is reduced to the study of theta-functions for $(\bar{H}, \bar{\alpha})$ on the quotient $\bar{V} = V/N$,

and we may restrict ourselves to the case when H is non-degenerate. In particular, we see that if H is degenerate with null space N, if θ vanishes at $z \in V$, it vanishes on the coset $z+N$, so that any section σ of $L(H, \alpha)$ which vanishes at an $x \in X = V/U$ also vanishes on the coset $x+X'$ where X' is the subtorus $N/U \cap N \subset X$. In particular, we see that if the sections of $L(H, \alpha)$ define a morphism of X into projective space at all, this morphism has to factor through the quotient torus X/X', $X' = N/U \cap N$. Thus $L(H, \alpha)$ cannot be ample if H is degenerate.

Next, suppose there is a complex subspace $W \subset V$ of positive dimension such that $H(w, w) < 0$ for $w \in W$, $w \neq 0$. Let K be a compact subset of V with $V = U + K$. Let $z_0 \in V$ and $w \in W$, and write $w = d+u$, $d \in K$, $u \in U$. We have

$$|\theta(z_0 + w)| = |\theta(z_0 + d + u)| = |\theta(z_0 + d)|\, e^{\pi \mathrm{Re} H(z_0+d,u)+\frac{1}{2}\pi H(u,u)}$$

and since

$$\begin{aligned}\mathrm{Re}H(z_0+d,u)+\tfrac{1}{2}H(u,u) &= \mathrm{Re}H(z_0+d,w)-\mathrm{Re}H(z_0+d,d)+\tfrac{1}{2}H(w,w)+\\ &\quad \tfrac{1}{2}H(d,d)-\mathrm{Re}H(w,d)\\ &= \tfrac{1}{2}H(w,w)+\mathrm{Re}\,H(z_0,w)+c(d,z_0).\end{aligned}$$

Of the terms on the right, for fixed z_0, the first is a real negative definite quadratic form in w, the second linear in w and the third is bounded (since d stays in a compact set K), so that the expression tends to $-\infty$ as $w \to \infty$ in W, and applying the maximum principle to $\theta(z_0 + w)$ as a function of w, we conclude that $\theta(z_0 + w) = 0$, hence $\theta \equiv 0$. Thus $L(H, \alpha)$ has no non-zero sections in this case. Therefore, if H is not positive definite, $L(H, \alpha)$ cannot be ample.

From now on, we work under the assumption that H is positive definite (and $E = \mathrm{Im}\, H$ integral on $U \times U$, as always). We shall prove the following

PROPOSITION. *When H is positive definite and $E = \mathrm{Im}\, H$ is expressed as a matrix using a basis of U over $\mathbf{Z}$, we have*

$$\begin{aligned}\dim H^0(X, L(H, \alpha)) &= \dim [\textit{space of theta-functions with respect to } (H, \alpha)]\\ &= +\sqrt{\det E}.\end{aligned}$$

PROOF. The idea of the proof is as follows. Since in $e_u(z)$, z occurs in the exponential linearly, one might hope that by multiplying θ by $e^{Q(z)}$ where Q is a suitable quadratic function one will be able to obtain periodicity for the new function with respect to a big sublattice U' of U. We can then expand this periodic function as a Fourier series, and the behavior of θ with respect to lattice points not in U' can be expressed in terms of the Fourier coefficients. This enables one to compute the number of linearly independent solutions.

Let then $e_u(z) = \alpha(u).e^{\pi H(z,u)+\frac{1}{2}\pi H(u,u)}$ as usual, and let θ be a holomorphic function on V satisfying $\theta(z+u) = e_u(z)\,\theta(z)$. If $B\colon V \times V \to \mathbf{C}$ is any complex symmetric bilinear form, and if we put $\theta^*(z) = e^{-\frac{1}{2}\pi B(z,z)}\,\theta(z)$, $\theta^*(z)$ satisfies the modified equation

$$\theta^*(z+u) = \alpha(u)\, e^{\pi(H-B)(z,u)+\frac{1}{2}\pi(H-B)(u,u)}\,\theta^*(z)$$

for all $u \in U$. Now, we can choose a sublattice U' of U of rank g ($= \dim V$) such that (1) $E(U' \times U') = 0$, and (2) if $W = \mathbf{R}.U'$, $W \cap U = U'$. Then $W \cap iW$ is a complex subspace of V on which E and hence H is identically 0. Since H is non-degenerate, $W \cap iW = (0)$, and so $V = W \oplus iW \simeq \mathbf{C} \oplus_{\mathbf{Z}} U' \simeq \mathbf{C} \otimes_{\mathbf{R}} W$. Since $E(W \times W) = 0$, H has a real symmetric restriction to W, and by the above, there is a unique symmetric complex bilinear B on V such that $B \mid W \times W = H \mid W \times W$. By $\mathbf{C}$-linearity in the first variable, $H(z, w) = B(z, w)$ for $w \in W$, $z \in V$. Since $E \mid U' \times U' = 0$, $\alpha \mid U'\colon U' \to \mathbf{C}_1^*$ is a homomorphism, and we can find a $\mathbf{C}$-linear form λ on V with λ real on W and $\alpha(u) = e^{2\pi i\lambda(u)}$ for $u \in U'$. The functional equation for θ^* shows then that $e^{-2\pi i\lambda(z)}.\theta^*(z)$ is periodic with respect to the lattice U'.

Let us write $\hat{U}' = \mathrm{Hom}_{\mathbf{Z}}(U', \mathbf{Z}) \subset \mathrm{Hom}_{\mathbf{C}}(V, \mathbf{C})$, and expanding $e^{-2\pi i\lambda(z)}.\theta^*(z)$ in a Fourier series, we obtain the expression

$$\theta^*(z) = \sum_{\chi \in \hat{U}'} c_\chi .\, e^{2\pi i(\chi(z)+\lambda(z))}. \tag{1}$$

Now, for any $u \in U$ and $u' \in U'$, $(H - B)(u', u) = \overline{H(u, u')} - B(u, u')$ $= -2i\ \mathrm{Im}\, H(u, u') = 2i\, E(u', u)$ and if $\hat{u} \in \hat{U}'$ is defined by $\hat{u}(u') = E(u', u)$ and extended $\mathbf{C}$-linearly to V we deduce that $(H - B)(z, u)$

$= 2i\,\hat{u}(z)$. Substituting the Fourier series (1) in the functional equation we get for any $u \in U$,

$$\sum_{\chi \in \hat{U}'} c_\chi \cdot e^{2\pi i[\chi(u)+\lambda(u)]} \cdot e^{2\pi i[\chi(z)+\lambda(z)]} = \alpha(u) e^{i\pi \hat{u}(u)} \sum_{\chi \in \hat{U}'} c_\chi \cdot e^{2\pi i[\chi(z)+\lambda(z)+\hat{u}(z)]}$$

and comparing coefficients,

$$c_\chi = \alpha(u) \cdot e^{i\pi \hat{u}(u) - 2\pi i[\chi(u)+\lambda(u)]} \cdot c_{\chi - \hat{u}}. \tag{2}$$

Thus, if M is the image of U under the homomorphism $U \to \hat{U}'$ given by $u \longmapsto \hat{u}$, we see that the c_χ are uniquely determined once they are specified for χ running through a system of representatives of $\hat{U}'/M$. (Note that if $u_1, u_2 \in U$ with $\hat{u}_1 = \hat{u}_2$, then $E(U', u_1 - u_2) = 0$ so $u_1 - u_2 \in U'$ and one checks that the relations (2) obtained with u_1 and u_2 for u are the same.) We shall check conversely that given any system $\{c_\chi\}_{\chi \in \hat{U}'}$ of constants satisfying (2), there exists a corresponding function, i.e. the series (1) is the Fourier series of a holomorphic function. It suffices to check the uniform absolute convergence of (1) on compact subsets of V. Fixing a $\chi_0 \in \hat{U}'$ it suffices to prove this for the solution c_χ such that $c_\chi = 0$ if $\chi - \chi_0 \notin M$ and $c_{\chi_0} = 1$. Writing $\chi = \chi_0 + \hat{u}$ for $\chi \in \chi_0 + M$, when z lies in a compact set $K \subset V$, the series (1) is majorized in absolute value by

$$\text{const.} \sum_{\hat{u} \in M} |\, c_{\chi_0 + \hat{u}}\,| \cdot e^{2\pi |\hat{u}(z)|},$$

hence by

$$\text{const.} \sum_{\hat{u} \in M} e^{\pi \operatorname{Im} \hat{u}(u) + A\,\|\hat{u}\|}$$

where $\|u\|$ denotes a suitable norm on M, and A a positive constant determined by χ_0, K, α and H. Since the sum $V = W \oplus iW$ is direct, we can find $\mathbf{R}$-linear maps $\phi, \psi\colon V \to W$ such that $z = \phi(z) + i\psi(z)$.

Since $\hat{u}$ is real on W and $E(W \times W) = 0$, we get

$$\operatorname{Im} \hat{u}(u) = \operatorname{Im}[\hat{u}(\phi(u)) + i\hat{u}(\psi(u))]$$

$$= \hat{u}(\psi(u))$$
$$= E(\psi(u), u)$$
$$= E(\psi(u), \phi(u) + i\psi(u))$$
$$= E(\psi(u), i\psi(u))$$
$$= -H(\psi(u), \psi(u)).$$

Further, $\psi(u) = 0 \iff u = \phi(u) \iff u \in W \iff \hat{u} = 0$, so that $\operatorname{Im} \hat{u}(u)$ is a negative definite quadratic form on M. Thus, the above series converges very rapidly.

We deduce that the dimension of the space of theta-functions for (H, α) is the index $\hat{U}'/M$.

Thus we have only to show that if U is a free abelian group of order $2g$, E a skew symmetric bilinear form on U into $\mathbf{Z}$ non-degenerate over $\mathbf{Q}$, U' a direct summand of U of rank g on which $E \equiv 0$ and n the order of the cokernel of the map $U \to \operatorname{Hom}_{\mathbf{Z}}(\hat{U}', \mathbf{Z})$ defined by $u \longmapsto E(\cdot, u)$, then $|\det E| = n^2$. This follows from the diagram

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & U' & \longrightarrow & U & \longrightarrow & U/U' & \longrightarrow & 0 \\
 & & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma & & \\
0 & \longrightarrow & (\widehat{U/U'}) & \longrightarrow & \hat{U} & \longrightarrow & \hat{U}' & \longrightarrow & 0
\end{array}$$

with exact rows and columns, the definitions of α, β, and γ being via E, using the fact that α and γ are transposes of each other up to sign, hence have cokernels of same orders, and the fact that β has a cokernel of order $|\det E|$.

We can now prove the main theorem of this section.

THEOREM OF LEFSCHETZ. *Let X be a complex torus V/U, H a hermitian form on V such that $E = \operatorname{Im} H$ is integral on $U \times U$, α a map $U \to \mathbf{C}_1^*$, with $\alpha(u_1 + u_2) = \alpha(u_1)\,\alpha(u_2) e^{i\pi E(u_1, u_2)}$ and $L = L(H, \alpha)$*

the associated line bundle on X. Then the following statements are equivalent.

(1) *Given any complex subtorus Y of X, there is an integer $N > 0$, a section σ of $L^{\otimes N}$ and two points $x_1, x_2 \in X$, $x_1 - x_2 \in Y$ such that $\sigma(x_1) = 0$, $\sigma(x_2) \neq 0$.*

(2) *The hermitian form H is positive definite.*

(3) *The space of holomorphic sections of $L^{\otimes n}$ give an imbedding of X as a closed complex submanifold in a projective space, for each $n \geq 3$.*

PROOF. We have already shown earlier that (1) $\Rightarrow$ (2), and (3) $\Rightarrow$ (1) is clear. It remains to assume (2), and deduce (3).

We use the expressions "theta-functions for (H, α)" and "section of $L(H, \alpha)$" interchangeably, making the identifications indicated earlier. We shall prove (3) for $n = 3$ (the cases $n > 3$ being proved quite similarly).

Firstly, if θ is a section of $L(H, \alpha)$ and $a, b \in V$, then $\theta(z-a).\theta(z-b).\theta(z+a+b)$ is a section of $L(3H, \alpha^3)$. In fact, on making the substitution $z + u$ for z in this function, it acquires a factor

$$\alpha(u)^3 \exp\{\pi H(z-a, u) + \pi H(z-b, u) + \pi H(z+a+b, u) + \frac{3\pi}{2} H(u,u)\} = \alpha(u)^3 e^{\pi.3H(z,u) + \frac{1}{2}\pi 3H(u,u)}$$

which proves the assertion. Hence, if $z_0 \in V$, there is a section ϕ of L^3 not vanishing at z_0. In fact, one has only to take a non-zero section θ of $L(H, \alpha)$, which exists by the Proposition, and then to choose $a, b \in V$ such that $\theta(z_0 - a) \neq 0$, $\theta(z_0 - b) \neq 0$ and $\theta(z_0 + a + b) \neq 0$, and put ϕ to be the product $\theta(z-a).\theta(z-b).\theta(z+a+b)$. Thus, if $\theta_0, \ldots, \theta_d$ is a basis of the sections of L^3, we get a well-defined holomorphic map

$$\Theta: X \longrightarrow \mathbf{P}^d$$

given, in terms of homogeneous coordinates, by

$$\Theta(\pi(z)) = (\theta_0(z), \theta_1(z), \ldots, \theta_d(z)) \in \mathbf{P}^d, \; z \in V.$$

Next, we prove that Θ is an injective map. If not, there exist $z_1, z_2 \in V$, $z_1 - z_2 \notin U$, and a non-zero constant $\gamma \in \mathbf{C}^*$ such that for

all theta-functions ϕ for $(3H, \alpha^3)$, we have $\phi(x_2) = \gamma\phi(x_1)$. In particular, for any $a, b \in V$ and any theta-function θ for (H, α) we have

$$\theta(z_1 - a)\theta(z_1 - b)\theta(z_1 + a + b) = \gamma\theta(z_2 - a)\theta(z_2 - b)\theta(z_2 + a + b).$$

We now consider both sides as functions of a (fixing b), and take logarithmic derivatives, so as to eliminate γ. Writing ω for the (meromorphic) differential $\frac{d\theta}{\theta}$, we obtain the relation

$$-\omega(z_1 - a) + \omega(z_1 + a + b) = -\omega(z_2 - a) + \omega(z_2 + a + b), \; a\, b \in V$$

which means that the differential $\omega(z_2 + z) - \omega(z_1 + z)$ is translation invariant in z, hence of the form $dl(z)$, where l is a $\mathbf{C}$-linear form on V. But then, this is also the differential of $\log \frac{\theta(z + z_2)}{\theta(z + z_1)}$, so that we obtain an identity

$$\theta(z + z_2) = A_1 . e^{l(z)} . \theta(z + z_1)$$

for some $A_1 \in \mathbf{C}^*$. Writing $\sigma = z_2 - z_1$, this may also be written as

$$\theta(z + \sigma) = A e^{l(z)} \theta(z)$$

with a fixed $A \in \mathbf{C}^*$. Making the substitution $z \longmapsto z + u$ $(u \in U)$, using the functional equation for θ and comparing the multiplicators on both sides, we get that

$$e^{\pi H(\sigma, u)} = e^{l(u)}, \; u \in U,$$

$$\text{or } \pi H(\sigma, u) - l(u) \in 2\pi i\mathbf{Z}, \; u \in U.$$

This implies that $\pi H(\sigma, u) - l(u) = \pi H(u, \sigma) - l(u) + \pi(H(\sigma, u) - H(u, \sigma)) = \pi H(u, \sigma) - l(u) + 2\pi i E(\sigma, u)$ takes only pure imaginary values for all $u \in V$, hence the same holds for $\pi H(u, \sigma) - l(u)$, and this being complex linear in u, we must have $\pi H(u, \sigma) = l(u)$ for all $u \in V$. But then it follows that $2\pi i . E(\sigma, u) \in 2\pi i\mathbf{Z}$ for $u \in U$, hence $\sigma \in U^\perp = \{x \in V \mid E(x, u) \in \mathbf{Z}, \; \forall\, u \in U\}$, which is a lattice in V containing U as a sublattice of finite index. Since $\sigma \notin U$ by assumption, $U + \mathbf{Z}\sigma \supsetneq U$, and the equation

$$\theta(z + \sigma) = A . e^{l(z)} . \theta(z) = A' . e^{\pi H(z,\sigma) + \frac{1}{2}\pi H(\sigma,\sigma)} . \theta(z)$$

shows that θ is actually a θ-function for the lattice $U + \sigma\mathbf{Z}$, the hermitian form H and a suitable multiplicator α' on $U + \mathbf{Z}\sigma$ extend-

ing α. Now, this must hold for any section θ of $L(H, \alpha)$, and the dimension of the space of such θ's is $\sqrt{(\det_U E)}$, the root of the determinant of E for the lattice U. On the other hand, if $U' = U + \mathbf{Z}\sigma \supsetneq U$, the dimension of the space of theta-functions for the lattice U' and H and any multiplicator α' is $\sqrt{(\det_{U'} E)}$, the root of the determinant of E on the lattice U'. But since we have evidently

$$\det_U E > \det_{U'} E,$$

and since there are only finitely many possible α''s extending α, it follows that almost all theta-functions for H, α and U are not theta-functions for H, α', and U' for any α'. This is a contradiction. Hence $\Theta\colon X \to \mathbf{P}^d$ is injective.

To complete the proof of the theorem, we have only to establish that Θ induces an injective map of tangent spaces at all points of X. If not, there is a $z_0 \in V$ and a tangent vector $\sum_1^g \alpha_i \frac{\partial}{\partial z_i}$ at z_0 with not all $\alpha_i = 0$ mapped into the 0 vector at $\Theta(\pi(z_0))$ in $\mathbf{P}^d$. There is then an $\alpha_0 \in \mathbf{C}$ such that for all $\phi \in \Gamma(X, L(3H, \alpha^3))$,

$$\alpha_0 \phi(z_0) + \sum_{i=1}^{g} \alpha_i \frac{\partial \phi}{\partial z_i}(z_0) = 0,$$

i.e.
$$D(\log \phi)(z_0) = -\alpha_0$$

for all ϕ as above, where $D = \sum_1^g \alpha_i \frac{\partial}{\partial z_i}$. Take

$\phi(z) = \theta(z - a)\theta(z - b)\theta(z + a + b)$ as before, with $a, b \in V$ and $\theta \in \Gamma(L(H, \alpha))$. If we put $f(z) = D(\log \theta)(z)$, we obtain

$$f(z_0 - a) + f(z_0 - b) + f(z_0 + a + b) = -\alpha_0$$

for all $a, b \in V$. One concludes easily that f is a linear (not necessarily homogeneous) function of z. Integrating the equation $f(z) = D(\log \theta)(z)$, we obtain that there is an $\alpha \in V$, $\alpha \neq 0$ such that for all $\lambda \in \mathbf{C}$, we have

$$\theta(z + \lambda\alpha) = e^{c\lambda^2 + \lambda f(z)} \cdot \theta(z)$$

for some constant c. One concludes as in the earlier step (by writing down the transformation formulae for both sides, for the substitution $z \longmapsto z + u$, $u \in U$) that for all $\lambda \in \mathbf{C}$, $\lambda\alpha$ belongs to the lattice $U^\perp = \{z \in V \mid E(u, z) \in \mathbf{Z}, \forall\ u \in U\}$. This is a contradiction.

We next recall some definitions.

Let X be an algebraic variety over $\mathbf{C}$. There is a canonically associated analytic space structure on the underlying set of X. We denote this analytic space by X_{hol}, and its structure sheaf by $\mathcal{O}_{X,\text{hol}}$. Often, we will not be so explicit, and talk of holomorphic functions on X, holomorphic maps from or into X, etc. Also, we shall say that an analytic space X is algebraic or algebraisable if there is an algebraic variety Y such that $Y_{\text{hol}} \cong X$. Note further that an algebraic variety X is complete if and only if X_{hol} is compact. (This is an easy consequence of Chow's lemma.)

We now recall the

THEOREM OF CHOW. *Let X be a complete algebraic variety and Y a closed analytic subset of X_{hol}. Then Y is Zariski closed in X.*

Chow proved the theorem for $X = \mathbf{P}^N$, but the above version follows immediately from this and Chow's lemma.

An easy consequence is that if X and Y are complete algebraic varieties and $f\colon X_{\text{hol}} \to Y_{\text{hol}}$ is a holomorphic map, then f considered as a map from X to Y is an algebraic morphism. To prove this, let Γ in $X_{\text{hol}} \times Y_{\text{hol}} = (X \times Y)_{\text{hol}}$ be the graph of f; it is a closed analytic subset, hence a closed algebraic subset of $X \times Y$. For every $(x, f(x)) \in \Gamma$, the projection $\Gamma \to X$ induces a local homomorphism of the algebraic local rings $\mathcal{O}_{x,X} \to \mathcal{O}_{(x,f(x)),\Gamma}$. Let $\mathcal{O}_1 = \mathcal{O}_{x,X}$, $\mathcal{O}_2 = \mathcal{O}_{(x,f(x)),\Gamma}$. Then I claim that $\mathcal{O}_1 \to \mathcal{O}_2$ is an isomorphism. First, use the fact that the projection $\Gamma \to X$ is proper and bijective: by Zariski's Main Theorem, this means that $\mathcal{O}_2$ is a finite $\mathcal{O}_1$-module. Let $\tilde{\mathcal{O}}_2 = \mathcal{O}_{(x,f(x)),\Gamma,\text{hol}}$ and $\tilde{\mathcal{O}}_1 = \mathcal{O}_{x,X,\text{hol}}$. Since $\Gamma \to X$ is an analytic isomorphism, we get a diagram:

$$\begin{array}{ccc} \mathcal{O}_1 & \longrightarrow & \mathcal{O}_2 \\ \downarrow & & \downarrow \\ \tilde{\mathcal{O}}_1 & \xrightarrow{\approx} & \tilde{\mathcal{O}}_2. \end{array}$$

In particular, $\mathcal{O}_1 \to \mathcal{O}_2$ is injective. If m_i = maximal ideal in $\mathcal{O}_i$, then dividing by m_i^2, we get

$$\begin{array}{ccc} \mathcal{O}_1/m_1^2 & \longrightarrow & \mathcal{O}_2/m_2^2 \\ \wr\downarrow & & \wr\downarrow \\ \tilde{\mathcal{O}}_1/m_1^2\,\tilde{\mathcal{O}}_1 & \xrightarrow{\approx} & \tilde{\mathcal{O}}_2/m_2^2\,\tilde{\mathcal{O}}_2 \end{array}$$

hence $m_2 = m_1\mathcal{O}_2 + m_2^2$. Therefore the $\mathcal{O}_2$-module $m_2/m_1\mathcal{O}_2$ becomes (0) after $\otimes_{\mathcal{O}_2}\ \mathcal{O}_2/m_2$: hence by Nakayama's lemma, $m_2 = m_1\mathcal{O}_2$. Therefore the $\mathcal{O}_1$-module $\mathcal{O}_2/\mathcal{O}_1$ becomes (0) after $\otimes_{\mathcal{O}_1}\ \mathcal{O}_1/m_1$: hence by Nakayama's lemma, $\mathcal{O}_2 = \mathcal{O}_1$. This shows that $\Gamma \to X$ is an algebraic isomorphism, hence that f is an algebraic morphism.

In particular, we see that a compact, complex space has *at most one algebraic structure.*† One further fact that we will need is that if X is a complete algebraic variety, every meromorphic function f

† For non-compact complex spaces, this is quite false. For instance, Serre [S1] p. 108, has given the following example: for every 1-dimensional abelian variety X over $\mathbf{C}$, there is a unique algebraic group G which is a non-trivial extension (as *alg.* group):

$$0 \longrightarrow \mathbf{C} \longrightarrow G \longrightarrow X \longrightarrow 0.$$

It is easily checked that if $\mathcal{O}_G$ is its (algebraic) structure sheaf, then $\Gamma(\mathcal{O}_G) = \mathbf{C}$. But taking the universal covering of G, one checks that analytically,

$$G = V/U,$$

V = a 2-dimensional complex vector space, $U = \{n_1\omega_1 + n_2\omega_2 | n_i \in \mathbf{Z}\}$ where ω_1, ω_2 are a $\mathbf{C}$-basis of V. If $\mathbf{G}_m$ denotes the 1-dimensional affine algebraic group, given by $\mathbf{C} - \{0\}$ under multiplication, it follows easily that G and $\mathbf{G}_m \times \mathbf{G}_m$ are two different algebraizations of the same analytic group!

on X_{hol} is a rational function on X, i.e. in the function field $\mathbf{C}(X)$; this can be proved similarly by considering the "graph" of f, and applying Chow's theorem.

Getting back to complex tori, we have

COROLLARY. *Let $X = V/U$ be a g-dimensional complex torus. The following are equivalent.*

(1) *X is the complex space associated to a projective algebraic variety,*

(2) *X is the complex space associated to any algebraic variety,*

(3) *there exist g algebraically independent meromorphic functions on X,*

(4) *there is a positive definite hermitian form H on V such that $\mathrm{Im}\,(H)$ is integral on $U \times U$.*

PROOF. (1) $\Rightarrow$ (2) $\Rightarrow$ (3) are obvious, (4) $\Rightarrow$ (1) has been proved in the theorem. It remains to prove (3) $\Rightarrow$ (4). Let $f_1, \ldots, f_g$ be the independent meromorphic functions. Let D_i be the polar divisor of f_i, $D = \Sigma D_i$, and L the line bundle associated to D. Then L admits $g+1$ sections $\sigma_0, \ldots, \sigma_g$ such that whenever f_i is regular, $\sigma_i = f_i\sigma_0$. By the theorem of Appell-Humbert, $L = L(H, \alpha)$ for some hermitian form H on V with $\mathrm{Im}\,H(U \times U) \subset \mathbf{Z}$, some α. Since L has sections at all, by the discussion preceding the theorem, we know that H is positive semi-definite. Let V_0 be its degenerate subspace, and $X_0 = V_0/V_0 \cap U$ the corresponding subtorus of X. Then the quotient torus X/X_0 equals $(V/V_0)/\mathrm{image}\,(U)$, and H is induced by a positive definite $\overline{H}$ on V/V_0, such that $\mathrm{Im}(\overline{H})$ is integral on the lattice $U/U \cap V_0$. Therefore, by the theorem, X/X_0 is a projective algebraic variety. But also, by the discussion earlier, we know that if σ is any section of L, the zeroes of σ are unions of cosets of X_0. Applying this to the sections $\sum_{i=1}^{g} \alpha_i\sigma_i$, it follows that all the analytic sets f_i = constant are unions of cosets of Y_0, hence each f_i is induced by a meromorphic function $\overline{f}_i$ on X/X_0. Let $\mathbf{C}(X/X_0)$ be the function field of X/X_0; then

$g = \text{tr. deg}_{\mathbf{C}}\, \mathbf{C}(\bar{f}_1, \ldots, \bar{f}_g) \leqslant \text{tr. deg}_{\mathbf{C}}\, \mathbf{C}(X/X_0) = \dim(X/X_0) < \dim X = g.$

Therefore $\dim X_0 = 0$, and H is non-degenerate.

As an example, notice that we get immediately the algebraizability of 1-dimensional tori: in fact, if $X = \mathbf{C}/\{n + m\omega / n, m \in \mathbf{Z}\}$, with $\text{Im}\ \omega > 0$, then let

$$H(z, w) = \frac{1}{\text{Im}\,(\omega)}\, z.\bar{w}.$$

One checks immediately that $\text{Im}\, H = E$ has values $E(1,1) = E(\omega, \omega) = 0$, $E(\omega, 1) = -E(1, \omega) = 1$, hence H satisfies the hypotheses of the theorem. Moreover, several projective embeddings of X are very well-known in the classical theory (cf. Hurwitz-Courant): for example, if

$$\mathfrak{p}(z) = \frac{1}{z^2} + \sum_{(n,m) \neq (0,0)} \left[\frac{1}{(z - n - m\omega)^2} - \frac{1}{(n + m\omega)^2} \right]$$

is the Weierstrass $\mathfrak{p}$-function, then $\mathfrak{p}$ is a meromorphic function, periodic with respect to $1, \omega$, with double poles at the points $n + m\omega$. The map:

$$z \longmapsto (1, \mathfrak{p}(z), \mathfrak{p}'(z)) \qquad \text{(projective coordinates)}$$

$$\mathbf{C} \longrightarrow \mathbf{P}^2$$

induces an isomorphism of X with a plane cubic curve of the form $X_0 X_2^2 = 4X_1^3 + aX_0^2 X_1 + bX_0^3$ (for suitable a, b depending on ω).

On the other hand, in dimensions $\geqslant 2$, it is easy to see that almost all tori are non-algebraic. In fact, we can check that on almost all tori X, $\text{Pic}(X) = \text{Pic}^0(X)$ or equivalently (by the theorem of Appell-Humbert) that there is no skew-symmetric $E = V \times V \to \mathbf{R}$ which is (a) integral on $U \times U$, and (b) satisfies $E(ix, iy) = E(x, y)$. Let $X = V/U$, and put $T = \text{Hom}_{\mathbf{C}}(V, \mathbf{C})$, $\overline{T} = \text{Hom}_{\mathbf{C}\text{-anti}}(V, \mathbf{C})$ as before. Consider the map

$$\begin{array}{ccc} \Lambda^2(\text{Hom}(U, \mathbf{Z})) & \hookrightarrow & \Lambda^2_{\mathbf{C}} \text{Hom}_{\mathbf{Z}}(U, \mathbf{C}) \\ & & \| \\ & & \Lambda^2_{\mathbf{C}} \text{Hom}_{\mathbf{R}}(V, \mathbf{C}) \\ & & \| \\ & & \Lambda^2_{\mathbf{C}}(T \oplus T) \simeq (\Lambda^2_{\mathbf{C}} T) \oplus (T \otimes \overline{T}) \oplus (\Lambda^2_{\mathbf{C}} \overline{T}). \end{array}$$

We want to show that for almost all lattices $U \subset V$ no element of $\Lambda^2_{\mathbf{Z}}(\text{Hom}(U, \mathbf{Z}))$ has image entirely in the middle factor $T \otimes \overline{T}$ on the right. It will suffice to show that $\Lambda^2_{\mathbf{Z}}(\text{Hom}\,(U, \mathbf{Z})) \to \Lambda^2_{\mathbf{C}} T$ is injective. But $\text{Hom}(U, \mathbf{Z})$ projects into a lattice in T, and for suitable choice of the lattice U in V, $\text{Im}\,(\text{Hom}(U, \mathbf{Z}))$ is an arbitrary lattice in T. So the conclusions follow from

LEMMA. *Let V be a g-dimensional complex vector space. Then for almost all lattices $U \subset V$, the map $\Lambda^g_{\mathbf{Z}} U \to \Lambda^g_{\mathbf{C}} V \simeq \mathbf{C}$ is injective (hence all the maps $\Lambda^k_{\mathbf{Z}} U \to \Lambda^k_{\mathbf{C}} V$ are injective, $k \leqslant g$).*

If coordinates $z_1, \ldots, z_g$ are introduced in V, and U is described by giving a basis $(\omega_{i1}, \ldots, \omega_{ig})$, $1 \leqslant i < 2g$, then almost all can be interpreted to mean all $g \times 2g$-tuples (ω_{ij}) not lying on a countable union of $(g(2g) - 1)$-dimensional analytic subsets. We leave the proof of this lemma to the reader.

II

ALGEBRAIC THEORY VIA VARIETIES

4. **Definition of abelian varieties.** We now turn to the study of abelian varieties over an arbitrary algebraically closed field k.

DEFINITION. *An abelian variety X is a complete algebraic variety*† *over k with a group law $m: X \times X \to X$ such that m and the inverse map are both morphisms of varieties.*

Note that if $k = \mathbf{C}$, then the underlying complex analytic space of an abelian variety is a compact complex analytic group, hence by the results of §1, it is a complex torus. When $k \neq \mathbf{C}$, the first aim of the theory of abelian varieties is to show that an abelian variety has properties analogous to those enjoyed by a complex torus. Of course, when char $k = 0$, many of these results can be proven by reduction to the case $k = \mathbf{C}$ (Lefschetz's principle), but when char $k \neq 0$, this is by no means possible. We shall want to answer the following basic questions.

QUESTION 1. Structure of X as an abstract group.

We will show that X is a commutative and divisible group. We will also show that if n_X denotes multiplication by n (n an integer > 0) on X, the kernel X_n of n_X, or what is the same, the group of elements $x \in X$ such that $nx = 0$, has the following structure :

$$X_n \simeq (\mathbf{Z}/n\mathbf{Z})^{2g} \text{ if char } k \nmid n,$$
$$X_{p^m} \simeq (\mathbf{Z}/p^m\mathbf{Z})^i \text{ if } p = \text{char } k,\ m > 0,$$

where i can take every value in the range $0 \leq i \leq g = \dim X$. This integer i will be called the *p-rank* of X.

QUESTION 2. Calculate the cohomology group $H^q(X, \Omega^p)$ (Ω^p being the sheaf of p-forms on X).

As in the classical cases we have canonical isomorphisms

$$H^q(X, \Omega^p) \simeq \overset{p}{\Lambda}[H^0(X, \Omega^1)] \otimes_k \overset{q}{\Lambda}[H^1(X, \mathcal{O}_X)],$$

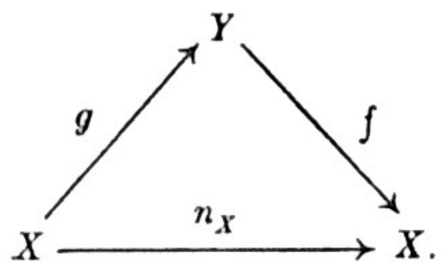
†This means, in particular, that it is irreducible.

and

$$\dim H^1(X, \mathcal{O}_X) = \dim H^0(X, \Omega^1) = g.$$

We also show that $\pi_1(X)$ (in the algebraic sense, i.e. the projective limit of finite groups of unramified Galois coverings) is isomorphic to $\prod_l (\mathbf{Z}_l)^{2g}$ in char 0 and to $\prod_{l \neq p} (\mathbf{Z}_l)^{2g} \times \mathbf{Z}_p^i$ in char p.

More precisely, we shall show that if $Y \xrightarrow{f} X$ is any morphism such that a finite group G acts freely on Y in such a way that X becomes the quotient of Y for this action, there is an integer $n > 0$ and a commutative diagram



Further, Y carries a structure of abelian variety such that f and g are homomorphisms.

QUESTION 3. The structure of Pic X.

We will show that there is an exact sequence

$$0 \longrightarrow \mathrm{Pic}^0 X \longrightarrow \mathrm{Pic}\ X \longrightarrow NS(X) \longrightarrow 0$$

where $\mathrm{Pic}^0 X$ has a natural structure of an abelian variety, and $NS(X)$ is a finitely generated free abelian group, whose rank ρ is called the *base number of* X.

We will also try to find analogues of the classical description of $NS(X)$ by Riemann forms E.

Related questions are: (a) for a pair of abelian varieties X, Y, show that $\mathrm{Hom}(X, Y)$ is a free abelian group on a finite number of generators, (here Hom means the set of maps which are both morphisms of varieties and homomorphisms of groups); and (b) give a matricial representation of this group of homomorphisms (in the classical case, we have the representation induced in $\mathrm{Hom}(H_1(X), H_1(Y))$).

QUESTION 4. Characterize ample line bundles. More generally, compute the cohomology groups of arbitrary line bundles, and in particular the dimension of the space of sections–this is the Riemann-Roch problem.

(i) We start with the observation that *an abelian variety is everywhere non-singular.* In fact, there has to exist a non-singular point $x_0 \in X$, and for $x \in X$, the translation morphism $T_{(x x_0^{-1})}$: $X \to X$, given by $T_{(x x_0^{-1})}(y) = x.x_0^{-1}.y$, is an automorphism of X carrying x_0 to x, so that x is again a non-singular point of X.

(ii) *As a group, X is commutative.* We give two proofs, one here and the second a little later. The first proof generalizes the proof we gave in the classical case. We consider not only the adjoint representation of X in the tangent space at the identity e, or in the space of differentials at e, but in each of the spaces $(\mathcal{O}_{X,e}/\mathfrak{M}_{X,e}^n)$ where $\mathcal{O}_{X,e}$ is the local ring of X at e and $\mathfrak{M}_{X,e}$ its maximal ideal. For $x \in X$, let $C_x: X \to X$ be defined by $C_x(y) = x\,y\,x^{-1}$, so that $C_x(e) = e$. Then C_x induces an automorphism $C_{x,n}^*$ of the vector space $\mathcal{O}_{X,e}/\mathfrak{M}_{X,e}^n$, deduced by passage to quotient from the automorphism $C_x^*: \mathcal{O}_{X,e} \to \mathcal{O}_{X,e}$ of the local ring. This induces a set theoretic map $\gamma: X \to \mathrm{Aut}(\mathcal{O}_{X,e}/\mathfrak{M}_{X,e}^n)$, $x \longmapsto C_{x,n}^*$ and if we put on the latter group the natural structure of an algebraic variety (viz. that induced from the inclusion $\mathrm{Aut}(\mathcal{O}_{X,e}/\mathfrak{M}_{X,e}^n) \subset \mathrm{End}(\mathcal{O}_{X,e}/\mathfrak{M}_{X,e}^n)$, the last being a finite-dimensional vector space over k), one checks easily that this is a morphism of varieties. Since the latter is an affine variety and X is complete and connected, γ must be a constant map! Since $\gamma(e)$ is the identity, we see that $C_{x,n}^*$ is the identity for all $x \in X$ and $n > 0$. But since $\bigcap_n \mathfrak{M}_{X,e}^n = (0)$ this means that $C_x^*: \mathcal{O}_{X,e} \to \mathcal{O}_{X,e}$ is the identity, so that C_x reduces to the identity in a neighbourhood of e in X. Since X is irreducible, C_x is the identity on X for every x, that is, X is commutative.

From now on, we write the group law in X additively. Moreover, we will use the following notations: for $x \in X$, we denote by

$T_x: X \to X$ the translation morphism $T_x(y) = x + y$; and the map $x \longmapsto n.x$ will be denoted by n_X.

(iii) *If $T = T_{X,0}$ is the tangent space at 0 to X, Ω_0 is the dual space $T^*_{X,0}$ of differentials, then there is a natural isomorphism*

$$\Omega_0 \otimes_k \mathcal{O}_X \xrightarrow{\sim} \Omega^1_X,$$

where Ω^1_X is the sheaf of regular 1-forms on X. One defines this mapping as follows. To each $\theta \in \Omega_0$, consider the 1-form ω_θ on X defined by $(\omega_\theta)_x = T^*_{-x}(\theta)$, that is, the unique translation invariant 1-form on X whose value at 0 is θ. It is checked easily that ω_θ is a regular 1-form on X. Thus, we have a natural homomorphism as above. Since at any point x, T^*_{-x} induces an isomorphism of the space of differentials at x onto the space Ω_0, it follows that the above homomorphisms of sheaves induces an isomorphism of fibers at x reduced modulo the maximal ideal $\mathfrak{M}_{X,x}$ at x. It follows by Nakayama's lemma that it is an isomorphism of sheaves.

Since X is complete and connected and $H^0(X, \mathcal{O}_X) = k$, it follows from the above isomorphism that the everywhere regular forms on X are precisely the invariant forms.

(iv) *For every n not divisible by the characteristic p of k, the endomorphism n_X is surjective.*

For the proof, we make the following observation. The tangent space $T_{X\times X,\,(0,\,0)}$ to $X \times X$ at $(0, 0)$ splits canonically into a direct sum $T_1 \oplus T_2$, where T_1 (resp. T_2) is the isomorphic image of $T_{X,0}$ under the immersion $X \to X \times X$ given by $x \xrightarrow{i_0} (x, 0)$ (resp. $x \xrightarrow{i_1} (0, x)$). Identifying T_i with $T_{X,0} = T$ by these isomorphisms, we note that the differential $d(m)$: $T \oplus T \to T$ of the addition map m: $X \times X \to X$, $m(x, y) = x + y$, is nothing but addition of components: $d(m)\,(t_1, t_2) = t_1 + t_2$. In fact, it is sufficient to check this (by linearity) on the two summands T of $T \oplus T$, and for these, it follows from the fact that the composites $X \xrightarrow{i_0} X\times X \xrightarrow{m} X$ and $X \xrightarrow{i_1} X\times X \longrightarrow X$ are the identity.

It follows by induction on n that for any $n > 0$ (and hence also for $n < 0$), $(dn_X)_0$ is multiplication by n. Thus, if $p \nmid n$, dn_X is an isomorphism. If n_X were not surjective, by the dimension theorem, $\dim_0 n_X^{-1}(0) > 0$, and we can therefore find a non-zero $t \in T$ tangent to $n_X^{-1}(0)$ at 0. But then, we would have $dn_X(t) = 0$ (since $n_X^{-1}(0)$ is mapped into the single point 0 by n_X), which is a contradiction.

The following lemma, besides having other important applications, gives a second proof of the commutativity of X.

RIGIDITY LEMMA. (Form I.) *Let X be a complete variety, Y and Z any varieties, and f: $X \times Y \to Z$ a morphism such that for some $y_0 \in Y$, $f(X \times \{y_0\})$ is a single point z_0 of Z. Then there is a morphism g: $Y \to Z$ such that if p_2: $X \times Y \to Y$ is the projection, $f = g \circ p_2$.*

PROOF. Choose any point $x_0 \in X$, and define $g : Y \to Z$ by $g(y) = f(x_0, y)$. Since $X \times Y$ is a variety, to show that $f = g \circ p_2$, it is sufficient to show that these morphisms coincide on some open subset of $X \times Y$. Let U be an affine open neighbourhood of z_0 in Z, $F = Z - U$, and $G = p_2\,(f^{-1}(F))$; then G is closed in Y since X is complete and hence p_2 is a closed map. Further $y_0 \notin G$ since $f(X \times \{y_0\}) = \{z_0\}$. Therefore $Y - G = V$ is a non-empty open subset of Y. For each $y \in V$, the complete variety $X \times \{y\}$ gets mapped by f into the affine variety U, and hence to a single point of U. But this means that for any $x \in X$, $y \in V$, $f(x, y) = f(x_0, y) = g \circ p_2(x, y)$, and this proves our assertion.

COROLLARY 1. *If X and Y are abelian varieties and f: $X \to Y$ is any morphism, $f(x) = h(x) + a$ where h is a homomorphism of X into Y and $a \in Y$.*

PROOF. Replacing f by $f - f(0)$, we may assume $f(0) = 0$ and we have to show under this assumption that f is a homomorphism.

Consider the morphism $X \times X \xrightarrow{\phi} Y$ defined by $\phi(x, y) = f(x + y) - f(y) - f(x)$. Then $\phi(X \times \{0\}) = \phi(\{0\} \times X) = 0$, so that it follows by the above lemma that $\phi \equiv 0$ on $X \times X$, or what is the same, that f is a homomorphism.

Note that in the proof of the above corollary, despite the additive notation used, no use of the commutativity of X was made. Thus, we may use it to give a second proof of the commutativity of X.

COROLLARY 2. *X is a commutative group.*

In fact, the morphism of X into itself mapping each element onto its inverse is a homomorphism by Corollary 1. Hence, for $x, y \in X$, $(xy)^{-1} = x^{-1}y^{-1} = y^{-1}x^{-1}$, and X is commutative.

COROLLARY 3. *Let X be an abelian variety (with base point 0). Then on the category of complete varieties with base point, the functor $S \longmapsto \mathrm{Hom}(S, X)$ (where Hom denotes morphisms preserving base point) is linear; that is, for S, T in this category, the natural map*

$$\mathrm{Hom}(S, X) \times \mathrm{Hom}(T, X) \longrightarrow \mathrm{Hom}(S \times T, X)$$

given by $(f, g) \longmapsto h$, $h(s,t) = f(s) + g(t)$ is a bijection.

PROOF. That this map is injective follows by fixing s and t in turn to be the base points s_0 and t_0 of S and T, respectively, in the equation $h(s, t) = f(s) + g(t)$. Next, take any $h \in \mathrm{Hom}(S \times T, X)$, and put $f(s) = h(s, t_0)$, $g(t) = h(s_0, t)$, $k(s, t) = h(s, t) - f(s) - g(t)$. Then $k(S \times \{t_0\}) = k(\{s_0\} \times T) = 0$, and it follows from the rigidity lemma that $k \equiv 0$.

APPENDIX TO §4

We want to prove the following result.

THEOREM. *Let X be a complete variety, $e \in X$ a point, and*

$$m: X \times X \longrightarrow X$$

a morphism such that $m(x, e) = m(e, x) = x$ for all $x \in X$. Then X is an abelian variety with group law m and identity e.

PROOF. We shall denote $m(x, y)$ simply by xy. Introduce the morphism

$$\psi: X \times X \longrightarrow X \times X$$

$$\psi: (x, y) = (xy, y).$$

Then $\psi^{-1}(e, e) = \{(e, e)\}$, so that by the dimension theorem, $\dim(\mathrm{Image}\,\psi) = \dim(X \times X)$. Since $X \times X$ is complete, this implies that ψ is surjective. In particular, given $x \in X$, there is an $x' \in X$ with $x'x = e$. Thus, if $\Gamma' = \{(x, y) \in X \times X \mid xy = e\}$, and $p_i (i = 1, 2)$ is the i^{th} projection of $X \times X$, $p_2(\Gamma') = X$. Choose an irreducible component Γ of Γ' with $p_2(\Gamma) = X$. Note that $\dim \Gamma \geqslant \dim X$. If $p_i' = p_i \mid \Gamma$, $p_1'^{-1}(e) = \{(e, e)\}$, so that again by the dimension theorem, $\dim(\mathrm{Image}\ p_1') = \dim X$. Since Γ is complete, this implies that p_1' is surjective.

Let $\phi: \Gamma \times X \to X$ be defined by $\phi((x', x), y) = x'(xy)$. Then $\phi(\Gamma \times \{e\}) = \{e\}$, so by the rigidity lemma, $\phi((x', x), y) = \phi((e, e), y)) = y$, that is,

$$x'(xy) = y, \quad \forall\ (x', x) \in \Gamma, \quad y \in X.$$

In particular, if $(x', x) \in \Gamma$, then $x'(x.x') = x'$. Choose an $(x'', x') \in \Gamma$, and multiply the last equation on the left by x'', to obtain

$$x''(x'(xx')) = x''x'.$$

But $x''x' = e$, and by (1), $x''(x'(xx')) = xx'$. Therefore if $(x', x) \in \Gamma$, then not only is $x'x = e$, but also $xx' = e$.

Let $\chi: \Gamma \times X \times X \to X$ be the map $\chi((x', x), y, z) = x((x'.y)z)$. Since $\chi(\Gamma \times \{e\} \times \{e\}) = e$, by the rigidity lemma,

$$x((x'\,y)z) = e((ey)z) = yz.$$

Multiplying on the left by x' and using (1), we get

$$(x'y)\,z = x'(x((x'y)z)) = x'(yz).$$

Since x' is arbitrary in X (p_1' being surjective), this shows that multiplication is associative. Thus X is a group with group law m. In particular, for any $x_0 \in X$, the translation $x \longmapsto x_0 x$ is an automorphism of X as a variety, and we deduce that X is non-singular. This also shows that ψ is bijective. But also the tangent map of ψ at (e, e) is an isomorphism since $\psi(x, e) = (x, e)$ and $\psi(e, x) = (x, x)$. Thus ψ cannot be inseparable, so that by Zariski's Main Theorem, ψ is an isomorphism. The inverse of ψ is given by $(x,y) \longmapsto (xy^{-1}, y)$, so this shows that $y \longmapsto y^{-1}$ is also a morphism, hence X is an abelian variety.

5. Cohomology and base change. At this point, we have to digress to prove a theorem of Grothendieck on the behavior of cohomology groups of a family of vector bundles E_y on a family of varieties X_y, parametrized by points $y \in Y$ where X_y is assumed to be a flat family of varieties. An important consequence of this result is the semicontinuity of the dimensions of the cohomology groups of the E_y.

We assume the following basic result.

THEOREM. *If $f: X \to Y$ is a proper morphism of locally noetherian preschemes and $\mathscr{F}$ a coherent sheaf of $\mathscr{O}_X$-modules on X, for all $p \geq 0$ the direct image sheaves $R^p f_*(\mathscr{F})$ are coherent sheaves of $\mathscr{O}_Y$-modules.*

We recall the following definition. If $f: X \to Y$ is a morphism of preschemes and $\mathscr{F}$ a quasicoherent sheaf on X, $\mathscr{F}$ is said to be *flat* over Y or *f-flat* if for each $x \in X$, $\mathscr{F}_x$(for its natural structure of $\mathscr{O}_{Y,f(x)}$-module) is $\mathscr{O}_{Y,f(x)}$-flat. It is easily shown that this condition is equivalent to requiring that for $U \subset X$, $V \subset Y$ with $U$and V affine open, and $f(U) \subset V$, $\mathscr{F}(U)$ is a flat $\mathscr{O}_Y(V)$-module.

The main result of this section is the following

THEOREM. *Let $f: X \to Y$ be a proper morphism of noetherian schemes with $Y = \operatorname{Spec} A$ affine, and $\mathscr{F}$ a coherent sheaf on X, flat over Y. There is a finite complex $K^\cdot: 0 \to K^0 \to K^1 \to \ldots \to K^n \to 0$ of finitely generated projective A-modules and an isomorphism of functors*

$$H^p(X \times_Y \operatorname{Spec} B, \mathscr{F} \otimes_A B) \cong H^p(K^\cdot \otimes_A B), \quad (p \geq 0)$$

on the category of A-algebras B.

PROOF. Choose a finite affine covering $\mathfrak{A} = \{U_i\}_{i \in I}$ of X by affine open subsets. Then the Čech complex $C^\cdot = C^\cdot(\mathfrak{A}, \mathscr{F}) = \oplus C^p(\mathfrak{A}, \mathscr{F})$ of alternating Čech cochains on $\mathfrak{A}$ with coefficients in $\mathscr{F}$ is a finite complex of A-flat modules, whose cohomologies are isomorphic to the cohomology groups $H^p(X, \mathscr{F})$.

Moreover, for all A-algebras B, $\{U_i \times_Y \operatorname{Spec} B\}$ is an affine covering of $X \times_Y \operatorname{Spec}(B)$, and $C^p(\mathfrak{A}, \mathscr{F}) \otimes_A B$ is the module of Čech p-cochains of $\mathscr{F} \otimes_A B$ for this covering. Therefore

$$H^p(X \times_Y \operatorname{Spec} B, \mathscr{F} \otimes_A B) \cong H^p(C^\cdot \otimes_A B)$$

for all B, and, in fact, functorially in B.

We need the following basic lemma

LEMMA 1. *Let $C^\cdot$ be a complex of A-modules (A any noetherian ring) such that the $H^i(C^\cdot)$ are finitely generated A-modules and such that $C^p \neq (0)$ only if $0 \leq p \leq n$. Then there exists a complex $K^\cdot$ of finitely generated A-modules such that $K^p \neq (0)$ only if $0 \leq p \leq n$ and K^p is free if $1 \leq p \leq n$ and a homomorphism of complexes $\phi: K^\cdot \to C^\cdot$ such that ϕ induces isomorphisms $H^i(K^\cdot) \xrightarrow{\sim} H^i(C^\cdot)$, all i. Moreover if the C^p are A-flat, then K^0 will be A-flat too.*

PROOF. We define, by descending induction on m, diagrams:

$$\begin{array}{ccccccccc}
K^m & \xrightarrow{\partial^m} & K^{m+1} & \xrightarrow{\partial^{m+1}} & K^{m+2} & \longrightarrow & \ldots & & \\
\downarrow{\scriptstyle \phi_m} & & \downarrow{\scriptstyle \phi_{m+1}} & & \downarrow{\scriptstyle \phi_{m+2}} & & & & \\
\ldots \longrightarrow C^{m-1} & \longrightarrow & C^m & \xrightarrow[\partial^m]{} & C^{m+1} & \xrightarrow[\partial^{m+1}]{} & C^{m+2} & \longrightarrow & \ldots
\end{array}$$

Put $K^p = 0$ for $p > n$. Suppose we have defined $(K^p, \phi_p, \partial^p)$ for $p \geq m+1$ such that the following conditions hold:

(i) $\partial^p \phi_p = \phi_{p+1} \partial^p$, $(p \geq m+1)$.

(ii) $\partial^{p+1} \circ \partial^p = 0$, $(p \geq m+1)$.

(iii) The ϕ^p induces isomorphisms in cohomology $H^q(K^\cdot) \xrightarrow{\sim} H^q(C^\cdot)$ for $q \geq m+2$, and a surjection $\ker \partial^{m+1} \to H^{m+1}(C^\cdot)$.

(iv) The K^p are A-free and finitely generated, $(p \geq m+1)$.

We then construct K^m, ∂^m and ϕ_m so as to satisfy (i)-(iii) with $m+1$ replaced by m.

Suppose first that $m \geq 0$. Let B^{m+1} be the kernel of the homomorphism $\ker \partial^{m+1} \to H^{m+1}(C^\cdot)$. Since B^{m+1} is finitely generated

over A (A being noetherian), we can find a finitely generated free module K'^m and a surjection $\partial': K'^m \to B^{m+1}$. Further, since $H^m(C^\cdot)$ is a finitely generated A-module, we can find a surjection $K''^m \xrightarrow{\lambda} H^m(C^\cdot)$ with K''^m finitely generated and free. Let $\mu: K''^m \to Z^m(C^\cdot)$ be any lift of λ, and $\phi''_m K''^m \to C^m$ the composite of μ with the inclusion $Z^m(C^\cdot) \to C^m$. We then put $K^m = K'^m \oplus K''^m$, and define $\partial^m: K^m \to K^{m+1}$ by putting it equal to zero on K''^m and equal to ∂' on K'^m. Since $\phi_{m+1} \circ \partial'(K'^m) \subset \partial C^m$, we can find $\phi'_m: K'^m \to C^m$ such that $\partial \circ \phi'_m = \phi_{m+1} \circ \partial'$. We then define $\phi_m: K^m \to C^m$ as being equal to ϕ'_m on K'^m and ϕ''_m on K''^m. The conditions (i)-(iii) are evidently fulfilled with m instead of $m+1$.

Suppose then that $m = -1$, that is, that $\{K^p, \phi_p, \partial^p\}$ have been defined for $p \geqslant 0$ satisfying (i)-(iii). We then replace K^0 by $K^0/\ker \partial^0 \cap \operatorname{Ker} \phi_0$, and we take $\phi_0: K^0 \to C^0$ and $\partial^0: K^0 \to K^1$ to be the induced mappings. Putting $K^p = 0$ for $p < 0$, we get a complex

$$0 \to K^0 \to K^1 \to K^2 \to K^3 \to \ldots \to K^n \to 0$$

and a homomorphism $\phi: K^\cdot \to C^\cdot$ which by construction induces isomorphisms in cohomology. We have only to check that K^0 is A-flat when all the C^p are A-flat. Consider the 'mapping cylinder' complex L defined by $L^p = K^p \oplus C^{p-1}$ for $p \in \mathbf{Z}$, and $\partial: L^p \to L^{p+1}$ defined by $\partial(x, 0) = (\partial x, \phi(x))$, $\partial(0, y) = (0, -\partial y)$. If $C''^\cdot$ is the complex obtained from $C^\cdot$ by shifting degrees by one (and making a sign change in ∂), $C'^p = C^{p-1}$, we have an exact sequence of complexes $0 \to C''^\cdot \to L^\cdot \to K^\cdot \to 0$, and hence an exact cohomology sequence

$$\begin{array}{ccccccccc} & & H^p(C^\cdot) & & & & H^{p+1}(C^\cdot) & & \\ & & \| & & & & \| & & \\ H^p(K^\cdot) & \longrightarrow & H^{p+1}(C''^\cdot) & \longrightarrow & H^{p+1}(L^\cdot) & \longrightarrow & H^{p+1}(K^\cdot) & \longrightarrow & H^{p+2}(C''^\cdot) \end{array}$$

and one sees from the definition that the cohomology maps $H^p(K^\cdot) \to H^{p+1}(C''^\cdot) \cong H^p(C^\cdot)$ are the ones induced by $\phi: K^\cdot \to C^\cdot$. Since these are all isomorphisms, $H^p(L^\cdot) = (0)$ for all $p \in \mathbf{Z}$. But

then $0 \to K^0 = L^0 \to L^1 \to L^2 \to \ldots \to L^{n+1} \to 0$ is exact and the modules L^i are flat for $i \geqslant 1$, hence K^0 is A-flat.

Applying the lemma to our case, we have a complex $K^\cdot$, and a homomorphism $K^\cdot \to C^\cdot$ such that

$$H^p(K^\cdot) \xrightarrow{\sim} H^p(C^\cdot) \simeq H^p(X, \mathscr{F}), \text{ all } p.$$

Note that K^0 is A-projective, since it is A-flat and finitely generated over a noetherian A. It remains to check that for all A-algebras B, $H^p(K^\cdot \otimes_A B) \to H^p(C^\cdot \otimes_A B)$ is an isomorphism too. This is a consequence of

LEMMA 2. *Let $C^\cdot$, $K^\cdot$ be any finite complexes of flat A-modules, and let $C^\cdot \to K^\cdot$ be a homomorphism of complexes inducing isomorphisms $H^p(C^\cdot) \xrightarrow{\sim} H^p(K^\cdot)$ for all p. Then for every A-algebra B, the maps $H^p(C^\cdot \otimes_A B) \xrightarrow{\sim} H^p(K^\cdot \otimes_A B)$ are isomorphisms.*

PROOF. Construct the 'mapping cylinder' $L^\cdot$ exactly as in the proof of Lemma 1. As before, we see that $L^\cdot$ is an exact finite complex of flat A-modules. Then it is easy to see that all the modules $Z^p = \operatorname{Ker}(L^p \xrightarrow{\partial^p} L^{p+1})$ are flat too, hence

$$0 \longrightarrow Z^p \longrightarrow L^p \longrightarrow Z^{p+1} \longrightarrow 0$$

is a short exact sequence of flat A-modules. Therefore

$$0 \longrightarrow Z^p \otimes_A B \longrightarrow L^p \otimes_A B \longrightarrow Z^{p+1} \otimes_A B \longrightarrow 0$$

is exact, from which it follows that $L^\cdot \otimes_A B$ is exact. But now $L^\cdot \otimes_A B$ is the mapping cylinder of the map $K^\cdot \otimes_A B \to C^\cdot \otimes_A B$. So using the cohomology sequence in reverse, it follows that $H^p(K^\cdot \otimes_A B) \to H^p(C^\cdot \otimes_A B)$ are isomorphisms.

For any morphism $f: X \to Y$ and $y \in Y$, we denote by X_y the fiber over y of f (i. e., the fiber product $X \times_Y \operatorname{Spec} k(y)$, considered as a scheme over $k(y)$), and for $\mathscr{F}$ quasi-coherent on X, we denote by $\mathscr{F}_y$ the sheaf $\mathscr{F} \otimes_{\mathscr{O}_Y} k(y)$ on X_y.

We have then the following important corollary.

COROLLARY. *Let X, Y, f and $\mathscr{F}$ be as in the theorem (except that Y need not be affine). Then we have:*

(a) *For each $p \geq 0$, the function $Y \to \mathbf{Z}$ defined by*

$$y \longmapsto \dim_{k(y)} H^p(X_y, \mathscr{F}_y)$$ *is upper semicontinuous on Y.*

(b) *The function $Y \to \mathbf{Z}$ defined by*

$$y \to \chi(\mathscr{F}_y) = \sum_{p=0}^{\infty} (-1)^p \dim_{k(y)} H^p(X_y, \mathscr{F}_y)$$

is locally constant on Y.

PROOF. The problem being local on Y, we may assume Y affine. Let $K^\cdot$ be a complex as in the proposition; by further localization, we may assume $K^\cdot$ to be a free complex. Denote by d^p: $K^p \to K^{p+1}$ the coboundary of K. We then have

$$\dim_{k(y)} H^p(X_y, \mathscr{F}_y) = \dim_{k(y)}[\ker (d^p \otimes_A k(y))] - \dim_{k(y)}[\mathrm{Im}(d^{p-1} \otimes_A k(y))]$$

$$= \dim_{k(y)}[K^p \otimes k(y)] - \dim_{k(y)}[\mathrm{Im}(d^p \otimes k(y))] - \dim_{k(y)}[\mathrm{Im}(d^{p-1} \otimes k(y))]. \quad (*)$$

The first term being constant on Y, (b) follows on taking alternating sum of (*) over all p. We assert that for any $p \geq 0$, the function $\rho_p(y) = \dim_{k(y)} [\mathrm{Im}(d^p \otimes k(y))]$ is lower semi-continuous on Y. In fact, if r is any integer ≥ 0, and $d_r^p: \Lambda^r K^p \to \Lambda^r K^{p+1}$ is the map induced by d^p,

$$\{y \in Y \mid \rho_p(y) < r\} = \{y \in Y \mid d_r^p \otimes k(y) = 0\},$$

and this set is closed since d_r^p is a homomorphism of free finitely generated modules, and hence is described by a matrix in A, and the above set is the set of common zeros of all entries of the matrix. This proves (a).

Moreover, the theorem gives the following criterion for putting together the cohomology groups of $\mathscr{F}$ along the fibres of f into a vector bundle on Y.

COROLLARY 2. *Let X, Y, f and $\mathscr{F}$ be as above. Assume Y is reduced and connected. Then for all p the following are equivalent:*

(i) $y \longmapsto \dim_{k(y)} H^p(X_y, \mathscr{F}_y)$ *is a constant function,*

(ii) $R^p f_*(\mathscr{F})$ *is a locally free sheaf $\mathscr{E}$ on Y, and for all $y \in Y$, the natural map*

$$\mathscr{E} \otimes_{\mathcal{O}_Y} k(y) \longrightarrow H^p(X_y, \mathscr{F}_y)$$

is an isomorphism.

If these conditions are fulfilled, we have further that

$$R^{p-1} f_*(\mathscr{F}) \otimes_{\mathcal{O}_Y} k(y) \longrightarrow H^{p-1}(X_y, \mathscr{F}_y)$$

is an isomorphism for all $y \in Y$.

PROOF. Again assume Y affine, $K^\cdot$ as in the proposition. (ii) $\Rightarrow$ (i) is obvious. To prove (i) $\Rightarrow$ (ii), we need two lemmas.

LEMMA 1. *If Y is reduced and $\mathscr{F}$ a coherent sheaf on Y such that $\dim_{k(y)}[\mathscr{F} \otimes_{\mathcal{O}_Y} k(y)] = r$, all $y \in Y$, then $\mathscr{F}$ is locally free of rank r on Y.*

PROOF. For any $y \in Y$, let $\sigma_1, \ldots, \sigma_r \in \mathscr{F}_y$ lift generators of $\mathscr{F}_y \otimes k(y)$. Since $\sigma_1, \ldots, \sigma_r$ are extendable to sections in a neighborhood of y, we have a homomorphism σ: $\mathcal{O}_Y{}^r|_V \to \mathscr{F}|_V$ defined in a neighborhood V of y. Then σ is surjective on the stalks at y, by Nakayama's lemma, so coker(σ) is zero at y and hence in a neighborhood of y. Thus, we may assume σ to be surjective. Then by assumption, for every $y' \in V$, the map

$$\sigma \otimes k(y')\text{: } k(y')^r \to \mathscr{F}_{y'} \otimes_{\mathcal{O}_{y'}} k(y')$$

is an isomorphism. Thus, if $\mathfrak{D}$ is the kernel of σ, we have $\mathfrak{D}_{y'} \subset \mathfrak{M}_{y'}\, \mathcal{O}_{y'}^r$ for each $y' \in V$. Since Y is reduced, this means that $\mathfrak{D} = (0)$. Thus σ is an isomorphism.

We apply this in the following

LEMMA 2. *Let Y be a reduced, noetherian affine scheme, and let*

$$\mathscr{F} \xrightarrow{\phi} \mathfrak{D}$$

be a homomorphism of coherent locally free $\mathcal{O}_Y$-sheaves. If $\dim_{k(y)}[\mathrm{Im}(\phi \otimes k(y))]$ *is locally constant, then there are splittings:*

$$\mathcal{F} \simeq \mathcal{F}_1 \oplus \mathcal{F}_2$$

$$\mathcal{D} \simeq \mathcal{D}_1 \oplus \mathcal{D}_2$$

such that $\phi \mid_{\mathcal{F}_1} = (0)$, $\mathrm{Im}(\phi) \subset \mathcal{D}_1$, *and* $\phi\colon \mathcal{F}_2 \to \mathcal{D}_1$ *is an isomorphism, i.e.*

$$\phi = \begin{bmatrix} 0 & \text{isom.} \\ 0 & 0 \end{bmatrix}.$$

PROOF. By Lemma 1, $\mathcal{D}/\phi(\mathcal{F})$ is locally free. If $Y = \mathrm{Spec}\,(A)$, $M = \Gamma(Y, \mathcal{F})$, $N = \Gamma(Y, \mathcal{D})$, then this means that $N/\phi(M)$ is A-projective. Therefore N splits into the direct sum of $\phi(M)$ and a second submodule isomorphic to $N/\phi(M)$. Or, in sheaves, $\mathcal{D} \simeq \mathcal{D}_1 \oplus \mathcal{D}_2$, where $\mathcal{D}_1 = \mathrm{Im}(\phi)$. Moreover, this shows that $\phi(M)$ is A-projective, too, so M splits into the direct sum of $\mathrm{Ker}(\phi)$ and a second submodule isomorphic to $\phi(M)$. Or, in sheaves, $\mathcal{F} \simeq \mathcal{F}_1 \oplus \mathcal{F}_2$, where $\phi(\mathcal{F}_1) = (0)$, $\phi\colon \mathcal{F}_2 \xrightarrow{\sim} \mathcal{D}_1$.

Now assume (i) holds. Let $K^\cdot$ be the complex given by the theorem. As in the proof of Corollary 1, $\dim[\mathrm{Im}(d^{p-1} \otimes k(y))]$ and $\dim[\mathrm{Im}(d^p \otimes k(y))]$ are locally constant. By Lemma 2, applied first to $d_p\colon K^p \to K^{p+1}$, and second to $d_{p-1}\colon K^{p-1} \to \mathrm{Ker}(d_p)$, we get splittings into projective modules:

$$\begin{array}{ccccc} Z_{p-1} \oplus K'_{p-1} & & B_p \oplus H_p \oplus K'_p & & B_{p+1} \oplus K'_{p+1} \\ \| & & \| & & \| \\ K_{p-1} & \longrightarrow & K_p & \longrightarrow & K_{p+1} \end{array}$$

where $Z_{p-1} = \mathrm{Ker}(d_{p-1})$, $d_{p-1}\colon K'_{p-1} \to B_p$ is an isomorphism, $B_p \oplus H_p = \mathrm{Ker}(d_p)$, and $d_p\colon K'_p \to B_{p+1}$ is an isomorphism. It follows immediately that

$$H^p(K^\cdot \otimes_A B) \simeq H_p \otimes_A B \simeq H^p(K^\cdot) \otimes_A B, \text{ all } B$$

and $H^{p-1}(K^\cdot \otimes_A B) \simeq Z_{p-1} \otimes_A B/\mathrm{Im}(d_{p-2} \otimes B) \simeq H^{p-1}(K^\cdot) \otimes_A B$, all B. This proves (ii).

COROLLARY 3. *Let X, Y, f and $\mathcal{F}$ be as above (unlike Corollary 2, Y need not be reduced). Assume for some p that $H^p(X_y, \mathcal{F}_y) = (0)$, all $y \in Y$. Then the natural map*

$$R^{p-1} f_*(\mathcal{F}) \otimes_{\mathcal{O}_Y} k(y) \to H^{p-1}(X_y, \mathcal{F}_y)$$

is an isomorphism for all $y \in Y$.

PROOF. Again assume $Y = \mathrm{Spec}\,(A)$, $K^\cdot$ as in the theorem. For all $y \in Y$, we know that

$$K^{p-1} \otimes k(y) \xrightarrow{d^{p-1}} K^p \otimes k(y) \xrightarrow{d^p} K^{p+1} \otimes k(y)$$

is exact. Split the vector space $K^p \otimes k(y)$ into $\overline{W}_1 \oplus \overline{W}_2$, where $\overline{W}_1 = \text{Image of } K^{p-1} \otimes k(y)$, and $\overline{W}_2$ is mapped injectively to $K^{p+1} \otimes k(y)$. To prove the corollary at y, we can replace A by any localization A_f, $(f \in A, f(y) \neq 0)$. If we do this for a suitable f, we may assume that K^p itself splits into a direct sum of free modules $W_1 \oplus W_2$ such that (a) $\overline{W}_i = W_i \otimes k(y)$, and (b) $W_1 \subset \mathrm{Im}(d^{p-1})$. To do this, just lift a basis of $\overline{W}_1$ to any elements in the image of d^{p-1}, and lift a basis of $\overline{W}_2$ arbitrarily. But then since $W_2 \otimes k(y) \to K^{p+1} \otimes k(y)$ is injective, it follows that $W_2 \to K^{p+1}$ is also injective if A is replaced again by a suitable localization A_f. But then $\mathrm{Im}(d^{p-1}) \cap W_2 = (0)$, hence $W_1 = \mathrm{Im}(d^{p-1})$. Since W_1 is a projective module the surjection $K^{p-1} \to W_1 \to 0$ splits, and $K^{p-1} \simeq \mathrm{Ker}(d^{p-1}) \oplus W_1$. It follows that we have exact sequences

$$K^{p-2} \longrightarrow \mathrm{Ker}(d^{p-1}) \longrightarrow H^{p-1}(X, \mathcal{F}) \longrightarrow 0$$

$$K^{p-2} \otimes k(y) \longrightarrow \mathrm{Ker}(d^{p-1}) \otimes k(y) \longrightarrow H^{p-1}(X_y, \mathcal{F}_y) \longrightarrow 0.$$

Therefore $H^{p-1}(X_y, \mathcal{F}_y) \simeq H^{p-1}(X, \mathcal{F}) \otimes k(y)$ as required.

COROLLARY 4. *Let X, Y, and $\mathcal{F}$ be as above. If $R^k f_*(\mathcal{F}) = (0)$ for $k > k_0$, then $H^k(X_y, \mathcal{F}_y) = (0)$ for all $y \in Y$, and for $k \geq k_0$.*

PROOF. Use Corollary 3 and decreasing induction on k_0.

COROLLARY 5. *Let X, Y, f and $\mathcal{F}$ be as above. Then if B is a flat A-algebra,*

$$H^p(X \times_Y \operatorname{Spec} B, \mathscr{F} \otimes_A B) \simeq H^p(X, \mathscr{F}) \otimes_A B.$$

PROOF. This follows immediately, from the fact that for B flat over A, and *any* complex $K^\cdot$,

$$H^p(K^\cdot \otimes_A B) \simeq H^p(K^\cdot) \otimes_A B.$$

COROLLARY 6. (Seesaw Theorem—provisional form). *Let X be a complete variety, T any variety and L a line bundle on $X \times T$. Then the set*

$$T_1 = \{t \in T \mid L|_{X \times \{t\}} \text{ is trivial on } X \times \{t\}\}$$

is closed in T, and if on $X \times T_1$, $p_2: X \times T_1 \to T_1$ is the projection, then $L|_{X \times T_1} \simeq p_2^* M$ for some line bundle M on T_1.

PROOF. We first make the remark that a line bundle M on a complete variety X is trivial if and only if $\dim H^0(X, \underline{M}) > 0$ and $\dim H^0(X, \underline{M}^{-1}) > 0$ where $\underline{M}$ denotes the sheaf of sections of M. In fact, the necessity of these conditions is clear. Suppose conversely that they hold. The first implies the existence of a non-zero homomorphism $\mathcal{O}_X \xrightarrow{\sigma} \underline{M}$, and the second implies a non-zero homomorphism $\mathcal{O}_X \to \underline{M}^{-1}$, hence on dualizing, a non-zero homomorphism $\underline{M} \xrightarrow{\tau} \mathcal{O}_X$. Hence $\tau(\sigma(1))$ is a non-zero section of $\mathcal{O}_X$, and since X is complete and connected, $\tau(\sigma(1))$ is a non-zero scalar. This implies that $\tau \circ \sigma$ is an isomorphism, hence σ and τ are isomorphisms.

It follows that T_1 is the set of points t of T such that $\dim H^0(X \times \{t\}, \underline{L}|X \times \{t\}) > 0$ *and* $\dim H^0(X \times \{t\}, \underline{L}^{-1}|X \times \{t\}) > 0$, and it follows from Corollary 1 that T_1 is closed. Replacing T by T_1 (so T is now merely a reduced scheme of finite type over k) and L by its restriction to $X \times T_1$, we may assume that $L \mid X \times \{t\}$ is trivial for each $t \in T$. Hence $\dim H^0(X \times \{t\}, L \mid X \times \{t\}) = 1$ for all $t \in T$, so that by Corollary 2, $p_{2*}(\underline{L}) = \underline{M}$ is an invertible sheaf on T and

$$\underline{M} \otimes_{\mathcal{O}_T} (kt) \leftarrow H^0(X \times \{t\}, \underline{L}|X \times \{t\})$$

is an isomorphism. It clearly follows from the triviality of $L|X \times \{t\}$ that the natural map $p_2^*(\underline{M}) \to \underline{L}$ is an isomorphism. Since $\underline{M}$ is the sheaf of sections of M, then $p_2^* M \simeq L$.

6. The theorem of the cube : I

THEOREM. *Let X, Y be complete varieties, Z any variety and x_0, y_0 and z_0 base points on X, Y, and Z, respectively. If L is any line bundle on $X \times Y \times Z$ whose restrictions to each of $\{x_0\} \times Y \times Z$, $X \times \{y_0\} \times Z$ and $X \times Y \times \{z_0\}$ are trivial, L is trivial.*

REMARK. Let T be a contravariant functor on the category of complete varieties into the category $\underline{\mathrm{Ab}}$ of abelian groups. Let $X_0, \ldots, X_n$ be any system of complete varieties, x_i^0 a base point of X_i, and let $\pi_i: X_0 \times \ldots \times X_n \to X_0 \times \ldots \times \hat{X}_i \times \ldots \times X_n$ ($\hat{X}_i$ indicating the omission of the i-th factor X_i) be the projection map, and $\sigma_i: X_0 \times \ldots \times \hat{X}_i \times \ldots \times X_n \to X_0 \times \ldots \times X_n$ the 'inclusion' defined by

$$\sigma_i(x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) = (x_0, \ldots, x_{i-1}, x_i^0, x_{i+1}, \ldots, x_n).$$

Consider the homomorphisms

$$\alpha_T^n: \prod_{i=0}^{n} T(X_0 \times \ldots \times \hat{X}_i \times \ldots \times X_n) \to T(X_0 \times \ldots \times X_n),$$

$$\beta_T^n: T(X_0 \times \ldots \times X_n) \to \prod_{i=1}^{n} T(X_0 \times \ldots \times \hat{X}_i \times \ldots \times X_n)$$

defined by

$$\alpha_T^n(\xi_0, \ldots, \xi_n) = \sum_0^n \pi_i^*(\xi_i), \ \beta_T^n(\eta) = (\sigma_0^*(\eta), \sigma_2^*(\eta), \ldots, \sigma_n^*(\eta)).$$

One then proves by an easy induction on n that we have a natural splitting $T(X_0 \times \ldots \times X_n) = \operatorname{Im} \alpha \oplus \operatorname{Ker} \beta$. The functor T is said to be of *order* n (*linear* if $n=1$, *quadratic* if $n=2$, etc.) if α is surjective, or equivalently β is injective. (Note that the definition of α is independent of base points.)

Thus, the above theorem (when Z is also assumed complete) may be paraphrased as saying that the functor $\operatorname{Pic} X$ is a quadratic functor on the category of complete varieties.

Now, if T_i $(1 \leqslant i \leqslant 3)$ are contravariant functors on complete varieties into Ab and $T_1 \xrightarrow{f} T_2$ and $T_2 \xrightarrow{g} T_3$ are natural transformations such that $T_1 \xrightarrow{f} T_2 \xrightarrow{g} T_3$ is an exact sequence, and if T_1 and T_3 are of order n, so is T_2, as follows from the exactness of

$$0=\operatorname{Ker}\beta^n_{T_1}(X_0,\ldots,X_n)\to\operatorname{Ker}\beta^n_{T_2}(X_0,\ldots,X_n)\to\operatorname{Ker}\beta^n_{T_3}(X_0,\ldots,X_n)=0.$$

Thus we get a proof of the theorem of the cube when the base field is **C** by observing that we have an exact sequence

$$H^1(X,\mathcal{O})\to H^1(X,\mathcal{O}^*)\to H^2(X,\mathbf{Z}),$$

functorial in X, and $H^1(X,\mathcal{O})$ is linear (hence quadratic) and $H^2(X,\mathbf{Z})$ is quadratic in X, by Künneth formulas.

Proof of the Theorem (following Weil and Murre). By the 'Seesaw theorem', it is sufficient to prove that for every $(x,z)\in X\times Z$, the restriction of L to $\{x\}\times Y\times\{z\}$ is trivial, since it is already given that L restricted to $X\times\{y_0\}\times Z$ is trivial. The following enables us to reduce the proof of the theorem to the case when X is a complete non-singular curve.

Lemma. *Let X be any variety and $x_0, x_1 \in X$. Then there is an irreducible curve C on X containing x_0 and x_1.*

Proof. We assume that $\dim X > 1$. By the lemma of Chow, we may assume X projective. Moreover, by induction on $\dim X$, it is sufficient to find a subvariety Y of codimension one in X containing x_0 and x_1. We can find an $X' \xrightarrow{f} X$ birational, with X' projective and $\dim f^{-1}(x_i) \geqslant 1$. (In fact, if h is any meromorphic function on X with indeterminacies at x_0 and x_1, X' can be taken to be the closure of the graph of h in $X\times\mathbf{P}^1$). If $X'\subset\mathbf{P}^N$ is an imbedding, there is a hyperplane H of $\mathbf{P}^N$ such that $H\cap X'=Y'$ is irreducible, by a theorem of Bertini, and $H\cap f^{-1}(x_i)\neq\emptyset$ since $\dim f^{-1}(x_i) > 1$. Then $Y=f(Y')$ is irreducible in X and contains x_0 and x_1, and the lemma is proved.

Resuming the proof of the theorem, we can find for any $x\in X$ an irreducible complete curve C_1 in X joining x_0 to x. Let $\pi: C\to C_1$ be the normalization of C_1 and $\pi': C\times Y\times Z\to X\times Y\times Z$ the induced map. The hypotheses of the theorem are clearly fulfilled for the bundle $\pi'^*(L)$ on $C\times Y\times Z$ (with X replaced by C and x_0 by any point of C lying over x_0), and it is sufficient to prove the triviality of this bundle, since it would then follow that L restricted to $\{x\}\times Y\times\{z\}$ is trivial for any $x\in X$ and $z\in Z$.

Thus, we assume X to be a complete non-singular curve, and it is even sufficient to show the existence of a non-void open subset Z' of Z such that L restricted to $X\times Y\times Z'$ is trivial, since we would then have proved the triviality of $L\mid X\times Y\times\{z\}$ for $z\in Z'$, and it would follow by continuity that this holds for all $z\in Z$.

Let Ω^1 be the sheaf of regular 1-forms on X and let $g=\dim H^0(X,\Omega^1)$ be the genus of X. We can clearly find g points $P_1,\ldots,P_g$ on X such that if $D=\sum_1^g P_i$, $\dim H^0(X,\Omega^1\otimes\mathcal{O}_X(-D))=0$. Denoting by p_1 the first projection $X\times Y\times Z\to X$, let L' be the line bundle $L'=L\otimes p_1^*(L_X(D))$ (where $L_X(D)$ is the line bundle associated to $\mathcal{O}_X(D)$) on $X\times Y\times Z$, and for any $(y,z)\in Y\times Z$, let $L'_{(y,z)}$ be the restriction of L' to $X\times\{y\}\times\{z\}$. Since $L'_{(y,z_0)}=L_X(D)$, we have $\dim H^1(X,\underline{L}'_{(y,z_0)})=\dim H^0(X,\Omega^1\otimes\mathcal{O}_X(-D))=0$ by Riemann-Roch so that the closed set $F=\{(y,z)\in Y\times Z\mid \dim H^1(X,\underline{L}'_{(y,z)})\geqslant 1\}$ of $Y\times Z$ does not encounter $Y\times\{z_0\}$. But Y being complete, we can find Z' open in Z and containing z_0 such that $Y\times Z'\cap F=\emptyset$, so that by restricting ourselves to Z', we may assume $H^1(X,\underline{L}'_{(y,z)})=0$ for all $(y,z)\in Y\times Z$. But this means that for all $(y,z)\in Y\times Z$,

$$\dim H^0(X,\underline{L}'_{(y,z)})=\chi(\underline{L}'_{(y,z)})=\chi(\underline{L}'_{(y_0,z_0)})=\chi(\mathcal{O}_X(D))=1-g+\deg D=1.$$

In view of Corollary 2 to the proposition if $p_{23}: X\times Y\times Z\to Y\times Z$ is the projection, $p_{23*}(\underline{L}')$ is an invertible sheaf on $Y\times Z$ of rank one and for any (y,z), the natural map $p_{23*}(\underline{L}')\otimes k(y,z)\to H^0(X,\underline{L}'_{(y,z)})$ is an isomorphism. Let U be any open subset of $Y\times Z$ on which $p_{23*}(\underline{L}')$ is trivial, and $\sigma_U\in\Gamma(U,p_{23*}(\underline{L}'))=\Gamma(p_{23}^{-1}(U),\underline{L}')$ a

generating section. Let $\widetilde{D}_U$ be the divisor of zeros of σ_U in $p_{23}^{-1}(U)$. Since for U,U' open in $Y \times Z$, σ_U and $\sigma_{U'}$ differ on $U \cap U'$ by a nowhere vanishing function, we have $\widetilde{D}_U \cap p_{23}^{-1}(U \cap U') = \widetilde{D}_{U'} \cap p_{23}^{-1}(U \cap U')$, so that we have an effective divisor $\widetilde{D}$ on $X \times Y \times Z$ such that $\widetilde{D} \mid p_{23}^{-1}(U) = \widetilde{D}_U$. For each $(y,z) \in Y \times Z$, the restriction of $\widetilde{D}$ to $X \times \{y\} \times \{z\}$ is the divisor of zeros of a non-zero section of $H^0(\underline{L}'_{(y,z)})$. In particular, $\widetilde{D}$ restricted to $X \times \{y\} \times \{z_0\}$ and $X \times \{y_0\} \times \{z\}$ for any $y \in Y, z \in Z$ must coincide with $D = \Sigma P_i$. Hence, if $P \in X$, $P \neq P_i (i = 1, \ldots, g)$, the restriction of $\widetilde{D}$ to $\{P\} \times Y \times Z$ has a support S not meeting $\{P\} \times Y \times \{z_0\}$ or $\{P\} \times \{y_0\} \times Z$. The projection T of S on Z is therefore a proper closed subset of Z, and since S is pure of codimension one in $\{P\} \times Y \times Z$, S must be of the form $\bigcup_{i=1}^{m} \{P\} \times Y \times T_i$, T_i closed and of codimension 1 in Z. But since $S \cap \{P\} \times \{y_0\} \times Z = \varnothing$, it follows that $S = \varnothing$, that is, the support of $\widetilde{D}$ does not meet $\{P\} \times Y \times Z$ for $P \in X$, $P \neq P_i$. Hence $\widetilde{D}$ must be of the form $\sum_1^g n_i(\{P_i\} \times Y \times Z)$, and restricting to $X \times \{y_0\} \times \{z_0\}$, we see that $\widetilde{D} = \sum_1^g (\{P_i\} \times Y \times Z)$. Hence for any $(y,z) \in Y \times Z$, $L'_{(y,z)}$ is the line bundle $L_X(D)$, and therefore L restricted to $X \times \{y\} \times \{z\}$ is trivial.

COROLLARY 1. *With X, Y, and Z as in the proposition, any line bundle on $X \times Y \times Z$ is isomorphic to $p_{12}^*(L) \otimes p_{13}^*(M) \otimes p_{23}^*(P)$ where p_{ij} is the projection of $X \times Y \times Z$ onto the product of the i^{th} and j^{th} factors, and L,M,P are line bundles on $X \times Y$, $X \times Z$, and $Y \times Z$, respectively.*

PROOF. This is a consequence of the remark preceding the proof of the theorem.

COROLLARY 2. *Let X be any variety, Y an abelian variety, and f,g,h: $X \to Y$ morphisms. Then for all $L \in \mathrm{Pic}(Y)$, we have*

$$(f+g+h)^*L \simeq (f+g)^*L \otimes (f+h)^*L \otimes (g+h)^*L \otimes f^*L^{-1} \otimes g^*L^{-1} \otimes h^*L^{-1}.$$

PROOF. Let $p_i : Y \times Y \times Y \to Y$ be the projection onto the i^{th} factor, put $m_{ij} = p_i + p_j : Y \times Y \times Y \to Y$ and $m = p_1 + p_2 + p_3$: $Y \times Y \times Y \to Y$.

Consider the line bundle

$$M = m^*L \otimes m_{12}^*L^{-1} \otimes m_{13}^*L^{-1} \otimes m_{23}^*L^{-1} \otimes p_1^*L \otimes p_2^*L \otimes p_3^*L$$

on $Y \times Y \times Y$. If q: $Y \times Y \to Y \times Y \times Y$ is the map $q(y,y') = (0,y,y')$, we have

$$q^*M = n^*L \otimes q_1^*L^{-1} \otimes q_2^*L^{-1} \otimes n^*L^{-1} \otimes 0^*L \otimes q_1^*L \otimes q_2^*L$$

where $0, q_1, q_2, n$: $Y \times Y \to Y$ are the 0 map, the projections, and addition. Therefore q^*M is trivial. By symmetry, M is trivial on $Y \times (0) \times Y$ and $Y \times Y \times (0)$ too. By the theorem, M must be trivial on $Y \times Y \times Y$. Pulling back M by the map (f,g,h): $X \to Y \times Y \times Y$, the result follows.

COROLLARY 3. *If X is an abelian variety, and $n \in \mathbf{Z}$, then for all line bundles L,*

$$n_X^*L \simeq L^{\left(\frac{n^2+n}{2}\right)} \otimes (-1_X)^*L^{\left(\frac{n^2-n}{2}\right)}.$$

PROOF. By Corollary 2 with $f = (n+1)_X$, $g = 1_X$ and $h = (-1)_X$, it follows that the "second difference",

$$(n+2)_X^*L \otimes (n+1)_X^*L^{-2} \otimes n_X^*L \simeq 1_X^*(L) \otimes (-1_X)^*L,$$

hence for some line bundles M_1, M_2, we must have

$$n_X^*L \simeq [L \otimes (-1_X)^*L]^{\frac{n(n-1)}{2}} \otimes M_1^n \otimes M_2.$$

Putting $n = 0$ shows that M_2 is trivial, and putting $n = 1$ shows $M_1 \simeq L$.

COROLLARY 4. (Theorem of the square.) *For all line bundles L $x,y \in X$,*

$$T_{x+y}^*L \otimes L \simeq T_x^*L \otimes T_y^*L.$$

Therefore if $\phi_L(x) =$ *isom. class of* $T_x^*L \otimes L^{-1}$ *in* $\mathrm{Pic}(X)$, ϕ_L *is a homomorphism from* X *to* $\mathrm{Pic}(X)$.

PROOF. Apply Corollary 2 with $X = Y$, f and g constant maps with images x, y respectively, and $h =$ identity.

In terms of divisors, Corollary 4 asserts that for any divisor D on X, and $x, y \in X$,

$$T_{x+y}^*D + D \equiv T_x^*D + T_y^*D$$

(where $\equiv$ means linear equivalence).

In the rest of this book, we will always keep the notation ϕ_L for this very important map. Note that

(a) $\phi_{L_1 \otimes L_2} = \phi_{L_1} + \phi_{L_2}$ ($+$ standing for the group law induced by $\otimes$ in $\mathrm{Pic}(X)$),

(b) $\phi_{T_x^*L} = \phi_L$.

DEFINITION. $K(L) = \mathrm{Ker}(\phi_L) = \{x \in X \mid T_x^*L \simeq L\}$.

PROPOSITION. *$K(L)$ is a Zariski-closed subgroup of X.*

PROOF. Apply the Seesaw Theorem to the line bundle $m^*L \otimes p_2^*L^{-1}$ on $X \times X$ ($m\colon X \times X \to X$ being addition). It follows that the set of $x \in X$ such that $m^*L \otimes p_2^*L^{-1}$ is trivial on $\{x\} \times X$ is Zariski closed. But $m^*L \otimes p_2^*L^{-1}\,|_{(x)\times X} \simeq T_x^*L \otimes L^{-1}$, so this set is $K(L)$.

APPLICATION 1. Let D be an effective divisor on an abelian variety X and $L = L(D)$ the associated line bundle. The following conditions are equivalent.

(i) The subgroup $H = \{x \in X \mid T_x^*(D) = D\}$ of X is finite (equality of divisors, not divisor classes).

(ii) $K(L)$ is finite.

(iii) The linear system $|2D|$ has no base points, and defines a finite morphism $X \to \mathbf{P}^N$.

(iv) L is ample on X.

PROOF. The implication (iii) $\Rightarrow$ (iv) is a general fact (*EGA* Ch. III, (2.6.1) or (4.4.2)). We show next that (iv) $\Rightarrow$ (ii). If $K(L)$ is not finite, let Y be the connected component of 0 of $K(L)$, so that Y is an abelian variety of positive dimension, and the restriction L_Y of L to Y is ample on Y. Further, $T_y^*(L_Y) \simeq L_Y$ for all $y \in Y$. Hence, by the Seesaw theorem if $m\colon Y \times Y \to Y$ is the addition and $p_i\colon Y \times Y \to Y$ the projections, the line bundle $m^*(L_Y) \otimes p_1^*(L_Y^{-1}) \otimes p_2^*(L_Y^{-1})$ is trivial on $Y \times Y$. Pulling back by the morphism $Y \to Y \times Y$, $y \longmapsto (y, -y)$ gives us that $L_Y \otimes (-1_Y)^*(L_Y)$ is trivial on Y. But L_Y is ample, and so is $(-1_Y)^*(L_Y)$ since -1_Y is an automorphism of Y, so that $L_Y \otimes (-1_Y)^*(L_Y)$ is again ample. This is a contradiction since $\dim Y > 0$, which proves that (iv) $\Rightarrow$ (ii). The implication (ii) $\Rightarrow$ (i) is trivial, since $K(L) \supset H$.

We now show that (i) $\Rightarrow$ (iii). The linear system $|2D|$ contains the divisors $T_x^*(D) + T_{-x}^*(D)$, by Corollary 4. For any $u \in X$, we can find an $x \in X$ such that $u \pm x \notin \mathrm{Supp}\ D$, and this means that $u \notin \mathrm{Supp}\ (T_x^*(D) + T_{-x}^*(D))$. Thus, the linear system $|2D|$ has no base points, and defines a morphism $\phi\colon X \to \mathbf{P}^N$. If ϕ is not a finite morphism, we can find an irreducible curve C such that $\phi(C) =$ one point. It follows that for all $E \in |2D|$, either E contains C or is disjoint from C. In particular, for almost all $x \in X$, C and $T_x^*(D) + T_{-x}^*(D)$ are disjoint. Now note the general fact.

LEMMA. *If C is a curve on X and E is an irreducible divisor on X such that $C \cap E = \emptyset$, then E is invariant under translation by $x_1 - x_2$, all $x_i \in C$.*

PROOF. If $L = L(E)$, then L is trivial on C since C and E are disjoint. Therefore, T_x^*L, restricted to C, has degree 0 for all $x \in X$. But then $T_x(C)$ and E can never intersect in a non-empty finite set of points, since this would imply that $T_x^*(L)\,|_C$ had positive degree; i.e. for all x, either $T_x(C)$ and E are disjoint, or $T_x(C) \subset E$. Let $x_1, x_2 \in C$, $y \in E$. Then $T_{y-x_2}(C)$ and E meet at y. Therefore $T_{y-x_2}(C) \subset E$, hence $y - x_2 + x_1 \in E$. This proves the lemma.

If $D = \Sigma n_i D_i$, D_i irreducible, then by the lemma, each D_i is invariant under translation by all points $x_1 - x_2$, $x_i \in C$. This contradicts (i), hence we have proved that (i) $\Rightarrow$ (iii).

This enables us to show trivially that an abelian variety X is projective. In fact, let U be any affine open subset of X, $D_1, \ldots, D_t$ the components of $X - U$ and D the divisor $D = \sum_1^t D_i$. We will show that D verifies (i) above. We may assume after a translation that $0 \in U$. Then $H = \{x \in X \mid T_x^*(D) = D\}$ is a closed subgroup, and for $x \in H$, U is stable for T_x. Since $0 \in U$, it follows that $H \subset U$, and H being complete and U affine, H is finite.

APPLICATION 2. An abelian variety X is a divisible group, and for all $n \geqslant 1$, X_n is finite.

Considering the homomorphism $n_X\colon X \to X$, it is clear that $\dim(\ker n_X) > 0$ if and only if $\dim(\mathrm{Im}(n_X)) < \dim X$. Hence to prove n_X surjective, it suffices to check that $X_n = \ker(n_X)$ is finite. But let L be an ample line bundle on X. Then

$$n_X^* L \simeq L^{\frac{n(n+1)}{2}} \otimes (-1_X)^* L^{\frac{n(n-1)}{2}}.$$

Since (-1_X) is an automorphism of X, $(-1_X)^*L$ is also ample, and since $\frac{1}{2}n(n+1) > 0$, $\frac{1}{2}n(n-1) \geqslant 0$, we see that n_X^*L is also ample. But then n_X^*L cannot be trivial on any positive dimensional subvariety. Since $n_X^* L|_{\mathrm{Ker}(n_X)}$ is trivial, $\ker(n_X)$ must be finite.

APPLICATION 3. We can go even further and compute the order of X_n, when the characteristic p of k does not divide n. We first recall some general facts. Let X and Y be complete varieties both of dimension n, and let $f\colon X \to Y$ be a surjective morphism. Then via f^*, $k(X)$ is a finite algebraic extension of $k(Y)$, and we define the *degree* d (resp. *separable degree*, *inseparable degree*) of f to be the degree $[k(X)\colon k(Y)]$ of this extension (resp. $[k(X)\colon k(Y)]_s$, $[k(X)\colon k(Y)]_i$). If f is separable, i.e. $k(X)$ is separable over $k(Y)$, then d is the cardinality of $f^{-1}(y)$ for almost all $y \in Y$. If f is inseparable, the separable degree of $k(X)$ over $k(Y)$ instead is the

cardinality of $f^{-1}(y)$ for almost all y. Moreover, a basic fact is that if $D_1, \ldots, D_n$ are Cartier divisors on Y, then we get the relation between intersection numbers:

$$(f^*D_1 \cdot \ldots \cdot f^*D_n)_X = d(D_1 \cdot \ldots \cdot D_n)_Y.$$

Now suppose X and Y are abelian varieties. A homomorphism $f\colon X \to Y$ is called an *isogeny* if it is surjective, with finite kernel. We have just seen that $n_X\colon X \to X$ is an isogeny. Then every isogeny f has a degree d, and since the cardinality of the kernel of f, $\#[\ker f]$, is the cardinality of $f^{-1}(y)$ for all $y \in Y$, we see that

$$\#[\ker f] = \text{separable degree } (f). \qquad (*)$$

Now take the case $f = n_X$. Let D be an ample, *symmetric* divisor (i.e. $(-1_X)^* D = D$) on X: we have seen that ample D's exist, and then $D + (-1_X)^*D$ is both ample and symmetric. Then by Corollary 3, n_X^*D is linearly equivalent to n^2D. Therefore, if $g = \dim X$,

$$\begin{aligned}\text{degree } (n_X) \cdot \overbrace{(D \cdot \ldots \cdot D)}^{g\times}{}_X &= \overbrace{(n_X^*D \cdot \ldots \cdot n_X^*D)}^{g\times}{}_X \\ &= n^{2g}\overbrace{(D \cdot \ldots \cdot D)}^{g\times}{}_X,\end{aligned}$$

hence degree $(n_X) = n^{2g}$.

When is n_X separable? If $p \nmid n$, then by the result above, $p \nmid$ degree (n_X) so n_X must be separable. On the other hand, if $p \mid n$, then we saw in § 4 that the differential $d(n_X)$ mapping $T_{X,0}$ to $T_{X,0}$ is 0. Therefore, if ω is any invariant differential form on X, $n_X^*(\omega)$ is (a) still translation invariant, and (b) has value 0 in the cotangent space to X at 0, hence it is zero. Since the invariant differentials on X generate the sheaf Ω_X^1 over $\mathcal{O}_X$, they generate the $k(X)$-module of $k(X)/k$-differentials. Therefore we find that the induced map n_X^* on rational differentials $\Omega^1_{k(X)/k}$ is 0 if $p \mid n$. This implies that the induced map on $k(X)$ maps $k(X)$ into $k(X)^p$, and hence the inseparable degree of p_X is at least p^g.

It follows that if $p \nmid n$, $\#(X_n) = n^{2g}$. Thus X_n is a finite abelian group killed by n such that for all $m \mid n$, X_n contains exactly m^{2g}

elements of order dividing m. It is elementary group theory that the only such group is $(\mathbf{Z}/n\mathbf{Z})^{2g}$. On the other hand, X_p is annihilated by p and is of order equal to the separable degree of p_X, which is p^i for some i with $0 \leqslant i \leqslant g$, so $X_p \simeq (\mathbf{Z}/p\,\mathbf{Z})^i$. Since X is divisible, it follows by induction on m that for any $m \geqslant 1$, $X_{p^m} \simeq (\mathbf{Z}/p^m\mathbf{Z})^i$. Summarizing, we have proved

PROPOSITION. (1) *degree* $(n_X) = n^{2g}$.

(2) n_X *separable* $\iff p \nmid n$.

(3) *If* $p \nmid n$, $X_n \simeq (\mathbf{Z}/n\mathbf{Z})^{2g}$.

(4) *There is an integer* i *with* $0 \leqslant i \leqslant g$ *such that for all* $m \geqslant 1$, $X_{p^m} \simeq (\mathbf{Z}/p^m\,\mathbf{Z})^i$.

APPENDIX TO §6

We give an alternative proof of the fact that $\deg n_X = n^{2g}$ for $n \geqslant 1$, avoiding intersection theory.

For an invertible sheaf $\underline{L}$ on a complete variety X of dimension g, and any coherent sheaf $\mathscr{F}$ on X, $P_{\mathscr{F}}(n) = \chi(\mathscr{F} \otimes \underline{L}^n)$ is a polynomial in n of degree $\leqslant g$. We shall denote the coefficient of n^g in this polynomial by $d_{\underline{L}}(\mathscr{F})/g!$, so that $d_{\underline{L}}(\mathscr{F})$ is an integer $\geqslant 0$. We call $d_{\underline{L}}(\mathscr{O}_X)$ the degree of $\underline{L}$, and denote it by $\deg \underline{L}$. The basic result is the following

PROPOSITION. (1) *Let* X *be a complete variety with an invertible sheaf* $\underline{L}$. *For any coherent sheaf* $\mathscr{F}$ *on* X, *let* $\operatorname{rank}(\mathscr{F})$ *be the dimension over the function field of* X *of the generic stalk of* $\mathscr{F}$, *or equivalently, of the space of rational sections of* $\mathscr{F}$. *Then we have*

$$d_{\underline{L}}(\mathscr{F}) = \operatorname{rank}(\mathscr{F}).\ \deg \underline{L}.$$

(2) *Let* $f: Y \to X$ *be a surjective morphism of complete varieties of the same dimension* g, *and* $\underline{L}$ *an invertible sheaf on* X. *Then*

$$\deg f^*(L) = (\deg f).(\deg L).$$

PROOF. (1) It is a standard fact that we can find a non-zero coherent sheaf of ideals $\mathscr{I}$ and an exact sequence

$$0 \longrightarrow \mathscr{I}^{\operatorname{rank}\mathscr{F}} \longrightarrow \mathscr{F} \longrightarrow \mathscr{T} \longrightarrow 0$$

with $\mathscr{T}$ a torsion sheaf. Since $\mathscr{T}$ has support of dimension $< \dim X$, $\chi(\mathscr{T} \otimes \underline{L}^n)$ is a polynomial of degree $< \dim X$, and the additivity of gives us that

$$d_{\underline{L}}(\mathscr{F}) = d_{\underline{L}}(\mathscr{I}^{\operatorname{rank}\mathscr{F}}) = (\operatorname{rank}\mathscr{F}).\, d_{\underline{L}}(\mathscr{I}),$$

and using the exact sequence $0 \to \mathscr{I} \to \mathscr{O}_X \to \mathscr{O}_X/\mathscr{I} \to 0$, we see that $d_{\underline{L}}(\mathscr{I}) = d_{\underline{L}}(\mathscr{O}) = \deg \underline{L}$.

(2) For each $p \geqslant 0$, we have a canonical isomorphism $R^p f_*(f^*(\underline{L}^n)) = R^p f_*(\mathscr{O}_Y) \otimes \underline{L}^n$. Taking alternating sums in the Leray spectral sequence $H^p(X, R^q f_*(f^*(\underline{L}^n))) \Rightarrow H^n(Y, f^*(\underline{L}^n))$, we obtain that

$$\chi(f^*(\underline{L}^n)) \equiv \sum_{p=0}^{\infty} (-1)^p\, \chi(R^p f_*(\mathscr{O}_Y) \otimes \underline{L}^n).$$

Since there is a non-void open subset U of X such that $f|f^{-1}(U): f^{-1}(U) \to U$ is a finite morphism, $R^p f_*(\mathscr{O}_Y)$ have supports in a proper closed subset of X for $p > 0$. Further, $R^0 f_*(\mathscr{O}_Y)$ is clearly a coherent sheaf of rank $= \deg f$. The assertion now follows on comparing coefficients of n^g on both sides.

Now let X be an abelian variety, n a positive integer. Let L be an ample symmetric line bundle on X; for any ample L, $L \otimes (-1_X)^* L$ is both ample and symmetric. Then by Corollary 3, $n_X^* L$ is isomorphic to L^{n^2}. Therefore, if $g = \dim X$, we get by the above proposition that

$$\deg n_X.\ \deg \underline{L} = \deg n_X^*(\underline{L}) = \deg \underline{L}^{n^2} = n^{2g}.\ \deg \underline{L},$$

and since $\deg \underline{L} > 0$, we get that $\deg n_X = n^{2g}$.

7. Dividing varieties by finite groups. Let $f: X \to Y$ be a morphism of algebraic varieties (over an algebraically closed field k). f is said to be *étale* if

(i) f is flat,

(ii) for all $x \in X$, $y = f(x) \in Y$, if m_x and m_y are the maximal ideals in $\mathcal{O}_x$ and $\mathcal{O}_y$, then $f^*(m_y)\mathcal{O}_x = m_x$.

This is equivalent to assuming that f is a "formal isomorphism" in the sense:

(i)′ for all $x \in X$, $y = f(x) \in Y$, if $\hat{\mathcal{O}}_x$, $\hat{\mathcal{O}}_y$ are the completions of $\mathcal{O}_x$, $\mathcal{O}_y$, then the natural map

$$\hat{f}^*: \hat{\mathcal{O}}_y \to \hat{\mathcal{O}}_x$$

is an isomorphism.

(Cf. Mumford, *Intro. Alg. Geom.*, p.353). When $k = \mathbf{C}$, it is also equivalent to assuming that f is a local isomorphism of analytic spaces. Our main result is

THEOREM. *Let X be an algebraic variety, and G a finite group of automorphisms of X. Suppose that for any $x \in X$, the orbit G_x of x is contained in an affine open subset of X. Then there is a pair (Y, π), where Y is a variety and $\pi: X \to Y$ a morphism, satisfying the following conditions:*

(i) *as a topological space, (Y, π) is the quotient of X for the G-action,*

(ii) *if $\pi_*(\mathcal{O}_X)^G$ denotes the subsheaf of G-invariants of $\pi_*(\mathcal{O}_X)$ for the action of G on $\pi_*(\mathcal{O}_X)$ deduced from* (i), *the natural homomorphism $\mathcal{O}_Y \to \pi_*(\mathcal{O}_X)^G$ is an isomorphism.*

The pair (Y, π) is determined up to an isomorphism by these conditions. The morphism π is finite, surjective and separable. Y is affine if X is affine.

If further G acts freely on X (that is, if $gx \neq x$ for any $x \in X$ and any $g \in G$ with $g \neq e$), π is an étale morphism.

PROOF. Since the conditions (i) and (ii) determine the topology and structure sheaf of Y, the uniqueness assertion is trivial. Also, the problem of existence reduces to proving that if Y is the quotient X/G as a topological space, and is given the structure sheaf $\mathcal{O}_Y = \pi_*(\mathcal{O}_X)^G$, it is an algebraic variety. Suppose we knew the theorem

(in its entirety) to be valid when X is affine. For any $x \in X$, let U' be an affine open subset of X containing Gx. Then $U = \bigcap_{g \in G} gU'$ is an affine open subset of X containing x and stable for G. Thus X is covered by G-stable affine open sets U. Then each $\pi(U)$ is open in Y, and $\pi^{-1}(\pi(U)) = U$, so by the affine case of the theorem $\pi(U)$, with the restriction of $\mathcal{O}_Y$, is an affine variety. But the open subsets $\pi(U)$ cover Y, so the theorem would follow for X.

We may therefore assume $X = \mathrm{Spec}(A)$. Let $A = k[x_1, \ldots, x_n]$. Then G acts on A by the law $g(f)(x) = f(g^{-1}x)$, $g \in G$, $f \in A$, $x \in X$. Let $\nu =$ order of G. For $f \in A$ and $1 \leqslant k \leqslant \nu$, denote by $\sigma_k(f)$ the elementary symmetric function of degree k in $\{g(f)\}_{g \in G}$, and put $B' = k[\sigma_i(x_j)]_{\substack{1 \leqslant i \leqslant \nu \\ 1 \leqslant j \leqslant n}}$, so that B' is a finitely generated k-algebra, contained in the algebra $B = A^G$ of G invariants of A. But the x_j are integral over B since they satisfy the equation

$$X^\nu - \sigma_1(x_j)X^{\nu-1} + \ldots + (-1)^\nu \sigma_\nu(x_j) = 0,$$

so A is a finite B'-module. Since $B' \subset B \subset A$ and B' is noetherian, B is a finite B'-module too and hence a finitely generated k-algebra, and A is a finite B-module. If $Y = \mathrm{Spec}\ B$, then Y is a variety and we get a morphism $\pi: X \to Y$ corresponding to the inclusion $B \subset A$, and this morphism is finite and surjective. Next if R is the quotient field of A, the action of G on A extends uniquely to an action on R. If $a/b \in R^G$, $a, b \in A$, $b \neq 0$, then

$$\frac{a}{b} = a \prod_{g \neq e} g(b) \Big/ \prod_{g \in G} g(b)$$

hence $a \cdot \prod_{g \neq e} g(b) \in A^G$, so that R^G is the quotient field of $A^G = B$. This proves that R is a Galois extension of the quotient field of B. In particular, π is separable. Next, note that $\pi_*(\mathcal{O}_X)^G$ is a coherent sheaf on Y since it is the intersection of kernels of

$$\phi_g: \pi_*(\mathcal{O}_X) \to \pi_*(\mathcal{O}_X),\ \phi_g(f) = gf,\quad f, g \in G.$$

The natural homomorphism $\mathcal{O}_Y \to \pi_*(\mathcal{O}_X)^G$ induces an isomorphism of global sections, so it is an isomorphism. Next if $x, x' \in X$ have distinct orbits $Gx \neq Gx'$ under G, we can find an $f \in A$ with

$f(gx) = 1$ for all $g \in G$, $f(gx') = 0$ for all $g \in G$, and if $\phi = \prod_{g \in G} g(f)$, $\phi \in B$ and $\phi(\pi(x)) = 1$, $\phi(\pi(x')) = 0$. This shows that $\pi(x) \neq \pi(x')$. Thus as a set, Y is the quotient of X by G. But $\pi: X \to Y$ is a finite and hence a closed and continuous map, so Y has the quotient topology too.

Only the last assertion remains to be checked. Let $x \in X$, $y = f(x)$, and $\mathfrak{M}$ the maximal ideal of y in B. Considering A as a B-module of finite type, let $\hat{B}$ and $\hat{A}$ be the completions of B and A respectively for the $\mathfrak{M}$-adic topology. Then, the natural homomorphism $\hat{B} \otimes_B A \to \hat{A}$ is an isomorphism. Moreover, $\hat{B}$ is also the completion $\hat{\mathcal{O}}_{Y,y}$ of $\mathcal{O}_{Y,y}$ with respect to its maximal ideal. On the other hand, since the only prime ideals of A containing $\mathfrak{M}.A$ are the maximal ideals of the points $g(x)$, $g \in G$, we have by the Chinese remainder theorem a natural isomorphism

$$\hat{A} \xrightarrow{\sim} \prod_{g \in G} \hat{\mathcal{O}}_{X,gx},$$

where $\hat{\mathcal{O}}_{X,gx}$ is the completion of $\mathcal{O}_{X,gx}$ with respect to its maximal ideal. The group G acts on A, and hence on the two other rings occurring above. On $\hat{B} \otimes_B A$, the action is given by $h(b \otimes a) = b \otimes h(a)$ for $h \in G$, $b \in B$, $a \in A$. The fact that B is the ring of G-invariants in A can be expressed by the exactness of the sequence of B-modules

$$0 \longrightarrow B \longrightarrow A \longrightarrow \prod_{h \in G} A$$

$$a \longmapsto (\ldots, h(a) - a, \ldots).$$

Since $\hat{B}$ is a flat B-module, it follows that

$$0 \longrightarrow \hat{B} \longrightarrow \hat{B} \otimes_B A \longrightarrow \prod_{h \in G} (\hat{B} \otimes_B A)$$

$$b \otimes a \longrightarrow (\ldots, b \otimes (h(a) - a), \ldots)$$

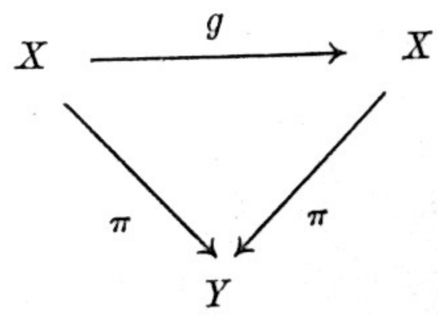
is exact, hence $\hat{B}$ is the subring of G-invariants in $\hat{B} \otimes_B A \simeq \hat{A}$. On the other hand, the action of $h \in G$ induces an isomorphism

$\hat{\mathcal{O}}_{X,x} \xrightarrow{\sim} \hat{\mathcal{O}}_{X,hx}$, and if we identify $\prod_{g \in G} \hat{\mathcal{O}}_{X,gx}$ with $\prod_{g \in G} \hat{\mathcal{O}}_{X,x}$ by means of these isomorphisms, the action of G on this ring may be described by simply permuting the factors, i.e. $h(\{\alpha_g\})_{g \in G} = \{\alpha_{(h^{-1}g)}\}_{g \in G}$, for any $h \in G$ and $\{\alpha_g\}_{g \in G} \in \prod_{g \in G} \hat{\mathcal{O}}_{X,x}$. Thus the invariants for this action can be identified with $\hat{\mathcal{O}}_{X,x}$, for its diagonal immersion in $\prod_{g \in G} \hat{\mathcal{O}}_{X,x}$. We thus deduce that the natural homomorphism $\hat{\mathcal{O}}_{Y,y} \to \hat{\mathcal{O}}_{X,x}$ is an isomorphism, i.e. f is étale at x.

REMARK. The condition that any G-orbit in X be contained in an affine open subset is always verified when X is quasi-projective. In fact, if X is a locally closed subset of $\mathbf{P}^N$ and if $\overline{X}$ is its closure in $\mathbf{P}^N$ and $x_i (1 \leqslant i \leqslant n)$ is any finite set of points of X, we can always find a hypersurface S in $\mathbf{P}^N$ containing $\overline{X} - X$ but not any of the x_i. Then $\overline{X} - (\overline{X} \cap S) = X - (X \cap S)$ is affine and open in X and contains all the x_i.

When X and G are as above and (Y, π) is the pair given by the theorem, Y is called the *quotient* of X by G, and is denoted by X/G.

Now let G act on X and let (Y, π) be the quotient, and let $\mathscr{F}$ be a coherent sheaf on Y. Since for any $g \in G$, we have the commutative triangle



we deduce that there is a natural automorphism $g^*: \pi^*(\mathscr{F}) \to \pi^*(\mathscr{F})$ over the action of g on X. Thus, G acts on $\pi^*(\mathscr{F})$ in a manner compatible with its action on X. By a coherent *G-sheaf* on X, we shall mean a coherent $\mathcal{O}_X$-module on which G acts in a way compatible with its action on X.

PROPOSITION 2. *Let G act freely on X, and $Y = X/G$. Then the functor $\mathcal{F} \longmapsto \pi^*(\mathcal{F})$ is an equivalence between the category of coherent $\mathcal{O}_Y$-modules and that of coherent G-sheaves on X, whose inverse is given by $\mathfrak{g} \to \pi_*(\mathfrak{g})^G$. Locally free sheaves correspond to locally free sheaves of the same rank.*

PROOF. There are natural homomorphisms

$$S(\mathcal{F})\colon \mathcal{F} \to \pi_*(\pi^*\mathcal{F})^G,\ \mathcal{F} \text{ a sheaf on } Y;$$

$$T(\mathfrak{g})\colon \pi^*(\pi_*(\mathfrak{g})^G) \to \mathfrak{g},\ \mathfrak{g} \text{ a } G\text{-sheaf on } X.$$

We will show that S and T are isomorphisms. We can again assume X and Y are affine. Let $X = \operatorname{Spec} A$, $Y = \operatorname{Spec} B$, where $B = A^G$. We must show that the natural maps

$$S(M)\colon M \to (M \otimes_B A)^G, \qquad M \text{ a } B\text{-module},$$

$$T(N)\colon (N^G) \otimes_B A \to N, \qquad N \text{ a } G\text{-}A\text{-module}$$

are isomorphisms. But for all B-modules M the composition

$$M \otimes_B A \xrightarrow{S(M) \otimes 1_A} (M \otimes_B A)^G \otimes A \xrightarrow{T(M \otimes_B A)} M \otimes_B A$$

is the identity. Since A is faithfully flat over B, $S(M) \otimes 1_A$ is an isomorphism if and only if $S(M)$ is an isomorphism; therefore it will suffice to prove that all the T's are isomorphisms.

Now in the case in which A is isomorphic as a ring to $B \times \ldots \times B$ and in which G acts on $B \times \ldots \times B$ by a simply transitive group of permutations, it is quite obvious that $T(N)$ is an isomorphism for every G-A-module N. On the other hand, we can reduce the proposition to this case by taking completions. Let $x \in X$, $y = f(x)$, and $\hat{B} = \hat{\mathcal{O}}_{y,Y}$. To show that $T(N)$ is an isomorphism, it will suffice to show that

$$[(N^G) \otimes_B A] \otimes_B \hat{B} \xrightarrow{T(N) \otimes 1_{\hat{B}}} N \otimes_B \hat{B}$$

is an isomorphism for every $y \in Y$. But since $\hat{B}$ is flat over B, the module of G-invariants in $N \otimes_B \hat{B}$ equals $(N^G) \otimes_B \hat{B}$ (cf. proof of theorem), hence we get a diagram

$$\begin{array}{ccc}
[N^G \otimes_B A] \otimes_B \hat{B} & \xrightarrow{T(N) \otimes 1_{\hat{B}}} & N \otimes_B \hat{B} \\
\wr\,\| & & \| \\
(N^G \otimes_B \hat{B}) \otimes_{\hat{B}} (A \otimes_B \hat{B}) & & \| \\
\wr\,\| & & \| \\
(N \otimes_B \hat{B})^G \otimes_{\hat{B}} (A \otimes_B \hat{B}) & \xrightarrow{T(N \otimes_B \hat{B})} & N \otimes_B B.
\end{array}$$

Since $A \otimes_B \hat{B}$ is isomorphic to $\prod_{g \in G} \hat{\mathcal{O}}_{g(x),X}$, hence to $\hat{B} \times \ldots \times B$, $T(N \otimes_B \hat{B})$ is an isomorphism.

We want to study in more detail the case when X is a complete variety and G acts freely on X. We shall denote by $\hat{G}$ the group $\operatorname{Hom}(G, k^*)$ of k^*-valued characters of G.

PROPOSITION 3. *In the above case, for all characters $\alpha\colon G \to k^*$, let*

$$\underline{L}_\alpha = \{a \in \pi_*(\mathcal{O}_X) \mid g(a) = \alpha(g).a, \text{ all } g \in G\}.$$

Then $\underline{L}_\alpha$ is an invertible sheaf on Y, and the multiplication in $\pi_*(\mathcal{O}_X)$ induces an isomorphism $\underline{L}_\alpha \otimes \underline{L}_\beta \to \underline{L}_{\alpha+\beta}$. The assignment $\alpha \longmapsto \underline{L}_\alpha$ defines an isomorphism

$$\hat{G} \xrightarrow{\sim} \operatorname{Ker}[\operatorname{Pic} Y \to \operatorname{Pic} X].$$

PROOF. By Proposition 2, $\operatorname{Ker}[\operatorname{Pic} Y \to \operatorname{Pic} X]$ can be identified as a set with actions of G on the trivial sheaf $\mathcal{O}_X$ covering the action of G on X. Given any such action, the image of the unit section by $g \in G$ is a nowhere vanishing section of $\mathcal{O}_X$, and since X is complete, a non-zero scalar $\alpha^{-1}(g) \in k^*$; clearly $\alpha\colon G \to k^*$ is a homomorphism. Conversely, given any such homomorphism, we can define an action of G on $\mathcal{O}_X$ covering the action on the base by $g(f) = \alpha^{-1}(g).(f \circ g^{-1})$. Thus, as a set, we have a bijection $\hat{G} \xrightarrow{\sim} \operatorname{Ker}[\operatorname{Pic} Y \to \operatorname{Pic} X]$. It is easy to see that this is a group homomorphism.

Given an action σ of G on $\mathcal{O}_X$ corresponding to a character α, if we denote the natural action of G on $\pi_*(\mathcal{O}_X)$ by $(g, f) \longmapsto g(f) = f \circ g^{-1}$, the action of G on $\pi_*(\mathcal{O}_X)$ induced by the action σ is described by

$$\sigma(g)(f) = \alpha^{-1}(g) \cdot g(f).$$

Since the corresponding invertible sheaf $\underline{L}_\alpha$ is the set of invariants of $\pi_*(\mathcal{O}_X)$ for this action, we get that

$$\underline{L}_\alpha \simeq \{a \in \pi_*(\mathcal{O}_X) \mid g(a) = \alpha(g).a\}.$$

Considered as subsheaves of $\pi_*(\mathcal{O}_X)$, we have evidently $\underline{L}_\alpha \cdot \underline{L}_\beta \subset \underline{L}_{\alpha+\beta}$. On the other hand, since a nowhere zero section on an open set of a line bundle on Y induces a nowhere zero section of the induced bundle on the inverse image of this open set, we see that any generating section $f \in \underline{L}_\alpha(U) \subset \Gamma(\pi^{-1}(U), \mathcal{O}_X)$ admits an inverse f^{-1} in $\pi_*(\mathcal{O}_X)(U)$, which clearly proves that $\underline{L}_\alpha \otimes \underline{L}_\beta \to \underline{L}_{\alpha+\beta}$ is surjective. Since both sides are invertible sheaves, this is an isomorphism.

REMARKS. (1) Suppose G is of order prime to the characteristic. Since the representations of G in all the k-vector spaces $\pi_*(\mathcal{O}_X)(V)$ are completely reducible for every open V in Y, it is easy to check that

$$\pi_*(\mathcal{O}_X) \simeq \bigoplus_{\alpha \in \hat{G}} \underline{L}_\alpha \oplus \mathcal{E}$$

where the representation of G in all the vector spaces $\mathcal{E}(V)$ contains no 1-dimensional subrepresentation. If G is also commutative, then we have simply

$$\pi_*(\mathcal{O}_X) \simeq \bigoplus_{\alpha \in \hat{G}} \underline{L}_\alpha.$$

Since $\pi_*\pi^*\mathcal{F} \simeq \mathcal{F} \otimes_{\mathcal{O}_Y} \pi_*\mathcal{O}_X$ for all $\mathcal{O}_Y$-modules $\mathcal{F}$, this proves also

COROLLARY. *If G has order prime to the characteristic, then for all coherent $\mathcal{O}_Y$-modules $\mathcal{F}$, $\mathcal{F}$ is a direct summand of $\pi_*(\pi^*\mathcal{F})$.*

Let us apply our results to abelian varieties. The main consequence is something like the fundamental theorem of Galois theory.

THEOREM 4. *Let X be an abelian variety. Then there is a* 1-1 *correspondence between the two sets of objects:*

(a) *finite subgroups $K \subset X$,*

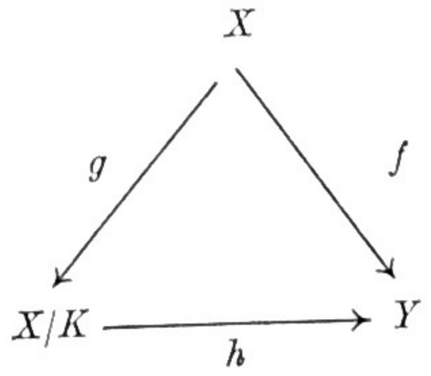
(b) *separable isogenies $f: X \to Y$, where two isogenies $f_1: X \to Y_1$, $f_2: X \to Y_2$ are considered equal if there is an isomorphism $h: Y_1 \to Y_2$ such that $f_2 = h \circ f_1$, which is set up by $K = \ker(f)$, and $Y = X/K$.*

PROOF. First start with a finite subgroup $K \subset X$. Then K acts freely on X by translations, so we can form the quotient $(X/K, f)$, and f is an étale surjective finite morphism $X \to X/K$. On the other hand, X/K as a set is the quotient of the abstract group X by the subgroup K, hence it has a group structure. The group law is in fact a morphism. This follows by considering the diagram:

$$\begin{array}{ccc} X \times X & \xrightarrow{\quad m \quad} & X \\ \downarrow{\scriptstyle f \times f} & & \downarrow{\scriptstyle f} \\ X/K \times X/K & \xrightarrow[\quad n \quad]{} & X/K \end{array}$$

where m is the group law of X (a morphism) and n is the group law of X/K (so far, just a map). But it is easy to check that $X/K \times X/K = X \times X/K \times K$, and since the morphism $f \circ m$: $X \times X \to X/K$ collapses the action of $K \times K$, it factors through $X \times X/K \times K$ i.e. n is also a morphism. Similarly, it can be checked that the inverse map on X/K is a morphism. Therefore X/K is an algebraic group. Finally, X/K is the image of a complete variety and therefore is complete. Thus X/K is an abelian variety, and $f: X \to X/K$ is a separable isogeny. Clearly the kernel of f is K.

Second, start with a separable isogeny $f: X \to Y$. Let K be its kernel, and as above form a new separable isogeny $g: X \to X/K$. A morphism h in the diagram:



exists, since f collapses the action of K, hence it factors through the quotient X/K. But h is obviously bijective, and the separability of f implies the separability of h. Therefore h is birational too. Therefore by Zariski's Main Theorem, h is an isomorphism.

COROLLARY 1. *A separable isogeny $f: X \to Y$ is an étale morphism.*

COROLLARY 2. *Let $f: X \to Y$ be an isogeny of order prime to p. Then the kernel of f and the kernel of f^*: $\mathrm{Pic}(Y) \to \mathrm{Pic}(X)$ are dual finite abelian groups.*

PROOF. Apply Proposition 3 and Theorem 4.

8. The dual abelian variety: char 0. We will use the hypothesis of char 0 only towards the end of this section.

DEFINITION. $\mathrm{Pic}^0(X)$ *is the subgroup of* $\mathrm{Pic}(X)$ *consisting of line bundles L such that the homomorphism ϕ_L is identically zero.*

By the theorem of the square, the *image* of each ϕ_L is contained in $\mathrm{Pic}^0(X)$, so we get an exact sequence:

$$0 \longrightarrow \mathrm{Pic}^0(X) \longrightarrow \mathrm{Pic}(X) \longrightarrow \mathrm{Hom}(X, \mathrm{Pic}^0(X)).$$
$$L \longmapsto \phi_L.$$

The main purpose of this section is to show (in char 0) that $\mathrm{Pic}^0(X)$ is naturally isomorphic to another abelian variety $\hat{X}$, called the dual of X. We make some general observations about $\mathrm{Pic}^0(X)$.

(i) $L \in \mathrm{Pic}^0(X) \Leftrightarrow T_x^* L \cong L$, all $x \in X$
$\Leftrightarrow m^*L \cong p_1^* L \otimes p_2^* L$ on $X \times X$.

PROOF. By the See-saw theorem, $m^*L \otimes p_1^* L^{-1} \otimes p_2^* L^{-1}$ is trivial if and only if it is trivial on $X \times \{a\}$ and on $\{0\} \times X$. But it always is trivial on $\{0\} \times X$ and its restriction to $X \times \{a\}$ is isomorphic to $T_a^* L \otimes L^{-1}$.

(ii) If $L \in \mathrm{Pic}^0(X)$, then for all schemes S and all morphisms $f, g: S \to X$, $(f+g)^*L \cong f^*L \otimes g^*L$.

PROOF. Consider the last isomorphism in (i) and pull it back to S by $(f, g): S \to X \times X$.

(iii) If $L \in \mathrm{Pic}^0(X)$, $n_X^* L \cong L^n$.

PROOF. Apply induction to (ii).

(iv) For all $L \in \mathrm{Pic}(X)$, $n_X^* L \cong L^{n^2} \otimes$ (something in $\mathrm{Pic}^0(X)$).

PROOF. In fact, by §6, $n_X^* L \cong L^{n^2} \otimes [L \otimes (-1_X)^* L^{-1}]^{(n-n^2)/2}$ so it suffices to prove that $L \otimes (-1_X)^* L^{-1} \in \mathrm{Pic}^0(X)$. By translating by x, we get

$$\begin{aligned} T_x^*(L \otimes (-1_X)^* L^{-1}) &\cong T_x^* L \otimes (-1_X)^* T_{-x}^* L^{-1} \\ &\cong T_x^* L \otimes (-1_X)^* \underbrace{[L \otimes T_{-x}^* L^{-1}]}_{\text{in } \mathrm{Pic}^0(X)} \otimes (-1_X)^* L^{-1} \\ &\cong T_x^* L \otimes L^{-1} \otimes T_{-x}^* L \otimes (-1_X)^* L^{-1}, \text{ by (iii)} \\ &\cong L \otimes (-1_X)^* L^{-1} \end{aligned}$$

by theorem of the square.

(v) If $L \in \mathrm{Pic}(X)$ has finite order, then $L \in \mathrm{Pic}^0(X)$.

PROOF. If L^n is trivial, $0 = \phi_{L^n}(x) = n\phi_L(x) = \phi_L(nx)$, all $x \in X$. Since X is divisible, this shows that $\phi_L \equiv 0$.

(vi) For all varieties S, and all line bundles L on $X \times S$, if $L_s = L|_{X \times \{s\}}$, then $L_{s_1} \otimes L_{s_0}^{-1} \in \mathrm{Pic}^0(X)$, $(s_0, s_1 \in S)$.

PROOF. Replacing S by open sets belonging to a covering of S, we can assume that $L|_{\{0\} \times S}$ is trivial. Further, replacing L by $L \otimes p_1^*(L_{s_0}^{-1})$, we can assume that L_{s_0} is trivial, and we must then prove that $L_s \in \mathrm{Pic}^0(X)$, all $s \in S$. We shall show that

$m^*(L_s) \otimes p_1^*(L_s^{-1}) \otimes p_2^*(L_s^{-1})$ is trivial for all s. In fact, construct a line bundle M on $X \times X \times S$

$$M = \mu^* L \otimes p_{13}^* L^{-1} \otimes p_{23}^* L^{-1},$$

$$\mu(x, y, s) = (x + y, s)$$

$$p_{13}(x, y, s) = (x, s)$$

$$p_{23}(x, y, s) = (y, s).$$

Then M is trivial on $X \times \{0\} \times S$, $\{0\} \times X \times S$ and $X \times X \times \{s_0\}$. Therefore by the theorem of the cube, M is trivial. But M, restricted to $X \times X \times \{s\}$ is $m^*(L_s) \otimes p_1^*(L_s^{-1}) \otimes p_2^*(L_s^{-1})$.

(vii) If $L \in \mathrm{Pic}^0(X)$ and L is not trivial, then $H^i(X, \underline{L}) = (0)$, all i.

PROOF. If $H^0(\underline{L}) \neq 0$, then $\underline{L} \simeq \mathcal{O}_X(D)$ for some non-negative divisor D. Then $\underline{L}^{-1} \simeq (-1_X)^* \underline{L} \simeq \mathcal{O}_X((-1_X)^* D)$, hence $\mathcal{O}_X \simeq \underline{L} \otimes \underline{L}^{-1} \simeq \mathcal{O}_X(D + (-1_X)^* D)$. Therefore $D + (-1_X)^* D = 0$, hence $D = 0$ and $\underline{L} \simeq \mathcal{O}_X$ which contradicts our assumption. This proves that $H^0(\underline{L}) = (0)$. Let k be the smallest integer such that $H^k(\underline{L}) \neq (0)$. Let $s_1 : X \to X \times X$ be the map $s_1(x) = (x, 0)$. Using the fact that $m^* L \simeq p_1^* L \otimes p_2^* L$ and the Künneth formula, we get the diagram:

$$\begin{array}{ccccc} X & \xrightarrow{s_1} & X \times X & \xrightarrow{m} & X \\ & \searrow & & & \\ H^k(X, \underline{L}) & \xleftarrow{s_1^*} & H^k(X \times X, m^* \underline{L}) & \xleftarrow{m^*} & H^k(X, \underline{L}) \\ & & \wr \| & & \\ & & H^k(X \times X, p_1^* L \otimes p_2^* \underline{L}) & & \\ & & \wr \| & & \\ & & \sum_{i+j=k} H^i(X, \underline{L}) \otimes H^j(X, \underline{L}). & & \end{array}$$

Since $m \circ s_1 = 1_X$, the dotted arrow is the identity. But if $i + j = k > 1$, then either $i < k$ or $j < k$, hence in all cases

$$H^i(X, \underline{L}) \otimes H^j(X, \underline{L}) = (0).$$

Therefore, the identity from $H^k(X, \underline{L})$ to $H^k(X, \underline{L})$ factors through a (0)-group. So $H^k(X, \underline{L}) = (0)$ too.

We now come to the really key point in the theory of Pic^0.

THEOREM 1. *Let L be ample and $M \in \mathrm{Pic}^0(X)$. Then for some $x \in X$,*

$$M \simeq T_x^* L \otimes L^{-1},$$

i.e. *the map $\phi_L : X \to \mathrm{Pic}^0(X)$ is surjective.*

PROOF. The whole idea is to look at the cohomology on $X \times X$ of the line bundle

$$K = m^* L \otimes p_1^* L^{-1} \otimes p_2^*(L^{-1} \otimes M^{-1}).$$

This cohomology is the abutment of two Leray spectral sequences associated to the two projections of $X \times X$ onto X:

(1) $H^l(X, R^k p_{1,*}(\underline{K})) \Rightarrow H^{k+l}(X \times X, \underline{K})$,

(2) $H^l(X, R^k p_{2,*}(\underline{K})) \Rightarrow H^{k+l}(X \times X, \underline{K})$.

Notice that on the fibres $\{x\} \times X$ of p_1 and $X \times \{x\}$ of p_2, K restricts to the line bundles

$$K|_{(x) \times X} \simeq T_x^* L \otimes L^{-1} \otimes M^{-1},$$

$$K|_{X \times (x)} \simeq T_x^* L \otimes L^{-1}.$$

Therefore, if $M \neq T_x^* L \otimes L^{-1}$ for any x, it follows that $K|_{(x) \times X}$ is a non-trivial line bundle in Pic^0 for every x. But by (vii), this means that all the cohomology groups of $K|_{(x) \times X}$ are (0). Therefore $R^k p_{1,*}(\underline{K}) = (0)$ for all k by Corollary 2, §5. Therefore $H^k(X \times X, \underline{K}) = (0)$ by spectral sequence (1).

Now use the other spectral sequence. Since $T_x^* L \otimes L^{-1}$ is non-trivial and in Pic^0 if $x \notin K(L)$, it follows that

$$\mathrm{supp}\,(R^k p_{2,*}(\underline{K})) \subset K(L).$$

Since $K(L)$ is a finite set, spectral sequence (2) degenerates to

$$\bigoplus_{x \in K(L)} R^k p_{2,*}(\underline{K})_x \simeq H^k(X \times X, \underline{K}).$$

But $H^k(X \times X, \underline{K}) = (0)$, so $R^k p_{2,*}(\underline{K}) = (0)$ too. Therefore $H^k(X, \underline{K}|_{X \times \{x\}}) = (0)$ for all x, by Cor. 4, § 5. But $K|_{X \times \{0\}}$ is the trivial line bundle, hence has a non-zero H^0! Thus we have a contradiction, so that the theorem must be true.

For a second proof of a slight weakening of the theorem, see Lang, p. 99. This important theorem shows that as an abstract group, $\mathrm{Pic}^0(X)$ is isomorphic to the abelian variety $X/K(L)$. If $\hat{X}$ is an abelian variety isomorphic as abstract group to $\mathrm{Pic}^0(X)$, what properties would we expect, which would characterize this "extra structure" on $\mathrm{Pic}^0(X)$?

(a) We want a line bundle P on $X \times \hat{X}$, the *Poincaré bundle* such that for all $\alpha \in \hat{X}$, the restriction P_α of P to $X \times \{\alpha\}$ represents the element of $\mathrm{Pic}^0(X)$ given by α under the isomorphism $\mathrm{Pic}^0(X) \simeq \hat{X}$. Moreover, we require that $P|_{\{0\} \times \hat{X}}$ is trivial. (These properties characterize P by the See-saw theorem.)

(b) For every normal variety S, and every line bundle K on $X \times S$ such that (i) $K_s = K|_{X \times \{s\}}$ is in $\mathrm{Pic}^0(X)$, for one and hence all $s \in S$, and (ii) $K|_{\{0\} \times S}$ is trivial, the unique set-theoretic map

$$f: S \to \hat{X}$$

such that $K_s \simeq P_{f(s)}$, is to be a morphism, and K is to be isomorphic to $(1_X \times f)^* P$.

It is easy to check that (a) and (b) uniquely characterize both $\hat{X}$ and P up to canonical isomorphisms. The problem is to construct such an $\hat{X}$ and P. So fix an ample L on X, and as suggested by the theorem, take $\hat{X}$ to be the quotient $X/K(L)$, constructed in §7. Let $\pi: X \to \hat{X}$ be the given morphism. To construct P, we shall use Prop. 2, §7. We want $(1_X \times \pi)^* P$ to be the line bundle $K = m^* L \otimes p_1^* L^{-1} \otimes p_2^* L^{-1}$ on $X \times X$. [This clearly should be the case: apply (b) with $S = X$, $K = m^* L \otimes p_1^* L^{-1} \otimes p_2^* L^{-1}$. Then $f = \pi$ so K should be isomorphic to $(1_X \times \pi)^* P$]. According to Prop. 2, we must lift the translation action of $\mathrm{Ker}(1_X \times \pi) = (0) \times K(L)$ on

$X \times X$, to an action of the same group on the line bundle K. But for any $a \in K(L)$, compute the pull-back $T^*_{(0,a)} K$:

$$\begin{aligned} T^*_{(0,a)} K &\simeq T^*_{(0,a)} m^* L \otimes T^*_{(0,a)} p_1^* L^{-1} \otimes T^*_{(0,a)} p_2^* L^{-1} \\ &\simeq m^* T_a^* L \otimes p_1^* L^{-1} \otimes p_2^* T_a^* L^{-1} \\ &\simeq m^* L \otimes p_1^* L^{-1} \otimes p_2^* L^{-1}, \end{aligned}$$

since $a \in K(L)$. Therefore, there is an automorphism $\phi_a: K \to K$ covering the automorphism $T_{(0,a)}: X \times X \to X \times X$ on the base space. However, each ϕ_a could be changed by a scalar, so there is no reason why $\phi_a \circ \phi_b = \phi_{a+b}$ should hold if the ϕ_a's are chosen arbitrarily. However, if $L^{-1}(0)$ is the fibre of the line bundle L^{-1} over 0, then notice that there is a *canonical* isomorphism:

$$\begin{aligned} K|_{\{0\} \times X} &\simeq m^* L|_{\{0\} \times X} \otimes p_1^* L^{-1}|_{\{0\} \times X} \otimes p_2^* L^{-1}|_{\{0\} \times X} \\ &\simeq L \otimes \begin{pmatrix} \text{trivial bundle} \\ L^{-1}(0) \times X \end{pmatrix} \otimes L^{-1} \\ &\simeq L^{-1}(0) \times X. \end{aligned}$$

Suppose we require that the automorphism ϕ_a of K should restrict on $\{0\} \times X$ to the product automorphism:

$$(\lambda, x) \longmapsto (\lambda, x + a)$$

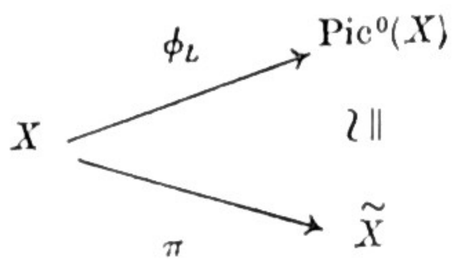
$$L^{-1}(0) \times X \to L^{-1}(0) \times X.$$

Clearly, there is a unique ϕ_a which has this restriction to $\{0\} \times X$. Since the restrictions then obey $\phi_a \circ \phi_b = \phi_{a+b}$, so do the ϕ_a's themselves. With this action of $\mathrm{Ker}(1_X \times \pi)$ on K, we construct a P on $X \times \hat{X}$ such that $(1_X \times \pi)^* P \cong K$.

Notice first that for all $\alpha \in \hat{X}$, if $\alpha = \pi(x)$, then

$$\begin{aligned} P_\alpha &\underset{\text{def}}{=} P|_{X \times \{\alpha\}} \\ &\simeq \pi^*(P)|_{X \times \{x\}} \\ &\simeq T_x^* L \otimes L^{-1}, \end{aligned}$$

i.e. P_α represents the element $\phi_L(x) \in \mathrm{Pic}^0(X)$. Therefore, if $\hat{X}$ is identified with $\mathrm{Pic}^0(X)$ so as to make the diagram



commute, the first part of (a) holds. Moreover, $P|_{\{0\}\times\hat{X}}$ is the quotient of $K|_{\{0\}\times X}$ by $\mathrm{Ker}(\pi)$, i.e. of $L^{-1}(0)\times X$ by the product action of $K(L)$. Therefore, $P|_{\{0\}\times\hat{X}} \simeq L^{-1}(0)\times\hat{X}$, a trivial bundle. Thus the second part of (a) holds.

To check that (b) holds, given S and K, consider the line bundle $E = p_{12}^*(K)\otimes p_{13}^*(P^{-1})$ on $X\times S\times\hat{X}$. Then $E|_{X\times\{\alpha,s\}} \simeq K_s\otimes P_\alpha^{-1}$, and the subset of $S\times X$:

$$\Gamma = \{\,(s,\alpha) \mid E|_{X\times(s,\alpha)} \text{ trivial}\,\}$$

is Zariski-closed in $S\times X$. But since $E|_{X\times(s,\alpha)}$ is trivial if and only if $K_s \simeq P_\alpha$, Γ is nothing but the graph of the set-theoretic map f. In particular, the projection $\Gamma\to S$ is a bijection. Now since the characteristic is 0†, this shows that Γ and S are birationally equivalent varieties, and since S is normal, $\Gamma\to S$ is an isomorphism of varieties by Zariski's Main Theorem. Therefore Γ is the graph of a morphism, i.e. f is a morphism. The last assertion in (b) follows from the See-saw theorem.

REMARKS. (1) For *every* line bundle L on X, the map $\phi_L: X\to\hat{X}$ is a morphism. This comes out of applying the universal mapping property (b) to the line bundle $m^*(L)\otimes p_1^*(L^{-1})\otimes p_2^*(L^{-1})$ on $X\times X$.

(2) If $X\xrightarrow{f} Y$ is a homomorphism of abelian varieties, the induced map $\mathrm{Pic}\ Y\to\mathrm{Pic}\ X$ maps $\mathrm{Pic}^0 Y$ into $\mathrm{Pic}^0 X$, and thus we get a natural map $\hat{f}: \hat{Y}\to\hat{X}$, and this is a morphism. In fact, if Q is the

†This is the only place where we use char. = 0! However, it is quite essential. The $\hat{X}$ we have constructed would definitely be "wrong" in char p.

Poincaré bundle on $Y\times\hat{Y}$, $(f\times 1)^*(Q)$ is a line bundle on $X\times\hat{Y}$ such that for $\hat{y}\in\hat{Y}$, $(f\times 1_{\hat{Y}})^*Q|_{X\times(\hat{y})}$ represents $f^*(\hat{y})\in\mathrm{Pic}^0 X$, and by the universal mapping property, $\hat{f}: \hat{Y}\to\hat{X}$ is a morphism.

(3) If $f: X\to Y$ is an isogeny, so is $\hat{f}: \hat{Y}\to\hat{X}$, and there is a canonical duality (of finite abelian groups) between $\mathrm{Ker} f$ and $\mathrm{Ker}\hat{f}$.

PROOF. We have seen in §7 that $\mathrm{Ker}(f)$ and $\mathrm{Ker}(f^*: \mathrm{Pic}(Y)\to\mathrm{Pic}(X))$ are dual. If $\hat{y}\in\mathrm{Pic}(Y)$ is such that $f^*(\hat{y})=0$, then this shows that $\hat{y}$ has finite order, hence $\hat{y}\in\mathrm{Pic}^0(Y)$. Therefore, $\mathrm{Ker}(f^*: \mathrm{Pic}\ Y\to\mathrm{Pic}\ X) = \mathrm{Ker}\hat{f}$. Finally, since $\dim\hat{X} = \dim X = \dim Y = \dim\hat{Y}$, it follows that $\hat{f}$ is an isogeny too.

The final point we want to make is that the relationship between X and $\hat{X}$ is in reality *symmetric* like the relationship between two vector spaces set up by a bilinear pairing. We can see this as follows.

DEFINITION. *Let X and Y be abelian varieties. A divisorial correspondence between X and Y is a line bundle Q on $X\times Y$ whose restrictions to $\{0\}\times Y$ and $X\times\{0\}$ are trivial.*

PROPOSITION 2. *Let X and Y be two abelian varieties of the same dimension, and Q a divisorial correspondence between X and Y. The following are equivalent*

(1) *If $Q|_{(x)\times Y}$ is trivial, then $x=0$,*

(2) *If $Q|_{X\times(y)}$ is trivial, then $y=0$.*

If these hold, then $X\simeq\hat{Y}$ with Q isomorphic to the Poincaré bundle P_Y of Y, and $Y\simeq\hat{X}$ with Q isomorphic to the Poincaré bundle P_X of X.

PROOF. By symmetry, it suffices to deduce (2) from (1). If (1) holds, there is an injective morphism $\phi: X\to\hat{Y}$ such that $Q\simeq(\phi\times 1_Y)^*P_Y$, P_Y being the Poincaré bundle on $\hat{Y}\times Y$. Since $\dim X = \dim\hat{Y}$ and ϕ is injective, ϕ is also surjective; since the characteristic is 0, this implies that ϕ is an isomorphism, i.e. $X\simeq\hat{Y}$.

Now, let $\psi: Y \to \hat{X}$ be the morphism such that if P_X is the Poincaré bundle on $X \times \hat{X}$, $(1_X \times \psi)^* P_X = Q$. To prove (2), we have to show that ψ is injective. If not, we can find a finite subgroup $K \subset \ker \psi$, $K \neq (0)$, and ψ factorizes as $Y \xrightarrow{\eta} Y/K \xrightarrow{\tilde{\psi}} \hat{X}$ where η is the natural homomorphism. Thus, if L is the line bundle $(1_X \times \tilde{\psi})^* P_X$ on $X \times Y/K$, we have that $Q \simeq (1_X \times \eta)^*(L)$. Now, L induces a homomorphism $\alpha: X \to (\widehat{Y/K})$, and the isomorphism $Q \simeq (1_X \times \eta)^*(L)$ means precisely that the composite $X \xrightarrow{\alpha} (\widehat{Y/K}) \xrightarrow{\hat{\eta}} \hat{Y}$ is the homomorphism defined by Q. Thus this composite is an isomorphism. Thus α is injective, and since $\dim X = \dim (\widehat{Y/K})$, α and $\hat{\eta}$ are both isomorphisms. But we know that $\hat{\eta}$ has a non-trivial kernel, viz. the dual abelian group of K. This is a contradiction, proving that ψ is injective.

9. The case $k = \mathbf{C}$. We want to link up the methods of Chapters 1 and 2 in this section. Therefore we assume that the ground field $k = \mathbf{C}$, and that $X = V/U$ (V a complex vector space, U a lattice) is an abelian variety over $\mathbf{C}$. Recall that every line bundle on X is isomorphic to $L(H, \alpha)$ for a unique Hermitian form H on V such that $E = \operatorname{Im} H$ is integral on $U \times U$, and a unique map $\alpha: U \to \mathbf{C}_1^*$ satisfying

$$\frac{\alpha(u_1 + u_2)}{\alpha(u_1)\alpha(u_2)} = e^{i\pi E(u_1, u_2)}, \quad u_1, u_2 \in U.$$

$L(H, \alpha)$ is, by definition, the quotient $(\mathbf{C} \times V)/U$ for the action

$$\phi_u(\lambda, z) = (\lambda . \alpha(u) . e^{\pi H(z,u) + \frac{\pi}{2} H(u,u)}, z + u).$$

We shall do two things: (A) compute $T^*_{\pi(x)}[L(H, \alpha)]$, $(x \in V)$, explicitly and hence interpret $\phi_{L(H,\alpha)}$ in the analytic case. (B) Describe divisorial correspondences as $L(H, \alpha)$'s and hence compute the dual $\hat{X}$ analytically.

(A) To keep the picture clear, it is convenient to generalize a little. Let a discrete group U act freely and discretely on V_1 and V_2 and let $T: V_1 \to V_2$ be a U-morphism. Let $X_i = V_i/U$, and let $\overline{T}: X_1 \to X_2$ be induced by T. Suppose U acts linearly on $\mathbf{C} \times V_2$ by

$$\phi_u(\lambda, z) = (\lambda . e_u(z), u(z)), \quad z \in V_2, \ \lambda \in \mathbf{C}, \ u \in U,$$

where $e_u(z)$ is a multiplicative co-cycle

$$e_{u_1 + u_2}(z) = e_{u_1}(u_2(z)) . e_{u_2}(z).$$

Let $L_2 = (\mathbf{C} \times V_2)/U$. Suppose we now want to describe the line bundle $L_1 = \overline{T}^*(L_2)$. Then

$$L_1 = X_1 \times_{X_2} L_2$$
$$\simeq [V_1 \times_{V_2} (\mathbf{C} \times V_2)]/U, \text{ where } U \text{ acts on both factors.}$$

Therefore, $L_1 = (\mathbf{C} \times V_1)/U$ with the action

$$\phi_u(\lambda, z) = (\lambda . e_u(Tz), u(z)), \ z \in V_1, \ \lambda \in \mathbf{C}, \ u \in U.$$

Now the co-cycle $\{e_u\}$ might be normalized to have a special form which $\{e_u \circ T\}$ might not have. Then we might use an automorphism of $\mathbf{C} \times V_1$:

$$(\lambda, z) \longmapsto (\lambda . g(z), z)$$
$$\mathbf{C} \times V_1 \longrightarrow \mathbf{C} \times V_1$$

and carrying over the action of U, obtain a new description of L_1 as $(\mathbf{C} \times V_1)/U$ with action

$$\phi_u(\lambda, z) = (\lambda e_u(T z) . g(u(z)) . g(z)^{-1}, u(z)).$$

Apply all this to the case $V_1 = V_2 = V$, $X_1 = X_2 = X$, T_a translation by $a \in V$, $\overline{T} = T_{\pi(a)}$ translation by $\pi(a)$, and $L_2 = L(H, \alpha)$. It follows that $T^*_{\pi(a)} L(H, \alpha)$ is $(\mathbf{C} \times V)/U$ with action

$$\phi_u(\lambda, z) = (\lambda . \alpha(u) . e^{\pi H(z+a,u) + \frac{1}{2}\pi H(u,u)}, z + u)$$
$$= (\lambda [\alpha(u) . e^{\pi H(a,u)}] . e^{\pi H(z,u) + \frac{1}{2}\pi H(u,u)}, z + u).$$

To simplify this co-cycle, take $g(z)$ to be the non-zero holomorphic function $e^{-\pi H(z,a)}$. We get the new action

$$\phi'_u(\lambda, z) = (\lambda . \alpha(u) . e^{\pi [H(a,u) - H(u,a)]} . e^{\pi H(z,u) + \frac{1}{2}\pi H(u,u)}, z + u)$$

and since $H(a, u) - H(u, a) = 2iE(a, u)$, we conclude:

PROPOSITION. $T^*_{\pi(a)}[L(H, \alpha)] \simeq L(H, \alpha \cdot \gamma_a)$ *where* $\gamma_a(u) = e^{2\pi i E(a,u)}$.

We get immediately lots of nice consequences.

(i) $\phi_{L(H,\alpha)}(\pi(a))$ is the point of $\mathrm{Pic}^0(X)$ represented by $L(0, \gamma_a)$.

(ii) In particular, since $\gamma_{a_1} \cdot \gamma_{a_2} = \gamma_{a_1+a_2}$, it follows that $\phi_{L(H,\alpha)}$ is a homomorphism; this is the theorem of the square.

(iii) We find

$$K(L(H, \alpha)) = U^\perp/U \subset V/U = X,$$

where $U^\perp = \{a | E(a, u) \in \mathbf{Z}, \text{ all } u \in U\}$.

(iv) Therefore $L(H, \alpha)$ is in $\mathrm{Pic}^0(X)$, as defined algebraically,

$\Leftrightarrow K(L(H, \alpha)) = X \Leftrightarrow U^\perp = V \Leftrightarrow E \equiv 0$

$\Leftrightarrow H \equiv 0$, i.e. $L(H, \alpha)$ is in $\mathrm{Pic}^0(X)$, as defined analytically.

(v) Moreover,

$K(L(H, \alpha))$ is finite $\Leftrightarrow U^\perp/U$ is finite

$\Leftrightarrow U^\perp$ is a lattice

$\Leftrightarrow E$ is non-degenerate

$\Leftrightarrow H$ is non-degenerate.

(vi) Notice that if H is non-degenerate, e.g. if $L(H, \alpha)$ is ample, then every homomorphism $U \to \mathbf{R}$ is given by $u \to E(a, u)$, for some $a \in V$. Therefore every homomorphism $\alpha : U \to \mathbf{C}_1^*$ is given by

$$u \to e^{2\pi i E(a,u)}$$

for some $a \in V$. Thus every element of $\mathrm{Pic}^0(X)$ is equal to $L(0, \gamma_a)$, some $a \in V$; this proves the main theorem of §8 when $k = \mathbf{C}$.

(B) Let $X_i = V_i/U_i$, $i = 1, 2$, be two abelian varieties. Then $Q = L(H, \alpha)$ on $X_1 \times X_2$ is a divisorial correspondence if Q is trivial on $\{0\} \times X_2$ and on $X_1 \times \{0\}$. This means that (a) the Hermitian form H is 0 on $\{0\} \times V_2$ and on $V_1 \times \{0\}$, and (b) $\alpha \equiv 1$ on $\{0\} \times U_2$ and on $U_1 \times \{0\}$. Define

$$B(x_1, x_2) = H((x_1, 0), (0, x_2)).$$

Then B is an $\mathbf{R}$-bilinear form on $V_1 \times V_2$, complex linear on V_1, and anti-linear on V_2. Let $\mathrm{Im}(B) = \beta$. Then β is integral on $U_1 \times U_2$, and we get

$$\begin{aligned} H((x_1, x_2), (y_1, y_2)) &= H((x_1, 0), (y_1, 0)) + H((x_1, 0), (0, y_2)) \\ &\quad + H((0, x_2), (y_1, 0)) + H((0, x_2), (0, y_2)) \\ &= B(x_1, y_2) + \overline{B(y_1, x_2)}. \\ \alpha((u_1, u_2)) &= \alpha((u_1, 0)) \cdot \alpha((0, u_2)) \cdot e^{\pi i E((u_1,0),(0,u_2))} \\ &= e^{\pi i \beta(u_1,u_2)}. \end{aligned}$$

Thus the divisorial correspondence Q is determined entirely by B.

In order to find the map from X_2 to $\hat{X}_1$ induced by Q, we next calculate the restriction of Q to $X_1 \times \{\pi_2(a_2)\}$, $a_2 \in V_2$. Let $Q' = (\mathbf{C} \times V_1 \times V_2)/U_1$. If $1 \times \pi_2 : X_1 \times V_2 \to X_1 \times X_2$ is the natural map, then $Q' \simeq (1 \times \pi_2)^* Q$, and $Q'|_{X_1 \times \{a_2\}} \simeq Q|_{X_1 \times \pi_2(a_2)}$. The action of U_1 on $\mathbf{C} \times V_1 \times V_2$ is given by

$$\phi'_{u_1}(\lambda, x_1, x_2) = (\lambda \cdot e^{\overline{\pi B(u_1, x_2)}}, x_1 + u_1, x_2).$$

Restricting to $V_1 \times \{a_2\}$, it follows that $Q'|_{X_1 \times \{a_2\}}$ equals $(\mathbf{C} \times V_1)/U_1$ with action

$$\phi''_{u_1}(\lambda, x_1) = (\lambda \cdot e^{\overline{\pi B(u_1, a_2)}}, x_1 + u_1).$$

Modifying this group action by the automorphism of $\mathbf{C} \times V_1$, scalar multiplication by $e^{-\pi B(x_1, a_2)}$, we get the action

$$\phi'''_{u_1}(\lambda, x_1) = (\lambda \cdot e^{-2\pi i \beta(u_1, a_2)}, x_1 + u_1).$$

Thus we have

PROPOSITION. $Q|_{X_1 \times \{\pi_2(a_2)\}} \cong L(0, \delta_{a_2})$ *where* $\delta_{a_2}(u_1) = e^{-2\pi i \beta(u_1, a_2)}$.

In particular, we see that in order that Q on $X_1 \times X_2$ satisfy the equivalent conditions of Proposition 2, §8, it is necessary and sufficient that $\dim X_1 = \dim X_2$ and that for all $x_2 \in V_2$, $x_2 \in U_2 \Leftrightarrow \beta(u_1, x_2) \in \mathbf{Z}$, all $u_1 \in U_1$. This implies that B is a non-degenerate pairing of V_1 and V_2. Hence,

COROLLARY. *Via* Q, $X_1 \simeq \hat{X}_2$ *and* $X_2 \simeq \hat{X}_1$ *if and only if*

(i) B *is non-degenerate*;

(ii) *under* β, U_1 *and* U_2 *are dual lattices, i.e.*

$$U_2 = \{x_2 \in V_2 \mid \beta(u_1, x_2) \in \mathbf{Z}, \text{ all } u_1 \in U_1\} \text{ and vice versa.}$$

Explicitly, therefore, if $X = V/U$, then the dual abelian variety $\hat{X}$ can be constructed as follows. Let

$$\overline{T} = \mathrm{Hom}_{\mathbf{C}\text{-antilinear}}(V, \mathbf{C}),$$

$$U' = \{l \in \overline{T} \mid \mathrm{Im}\, l(u) \in \mathbf{Z}, \text{ all } u \in U\}.$$

Then $X = \overline{T}/U'$. The form $B\colon V \times \overline{T} \to \mathbf{C}$ is simply $B(x, l) = \overline{l(x)}$, and the Poincaré bundle P_X on $X \times \hat{X}$ is simply $L(H, \alpha)$ with

$$H((x_1, l_1), (x_2, l_2)) = \overline{l_2(x_1)} + l_1(x_2)$$

$$\alpha((u, l)) = e^{-\pi i \,\mathrm{Im}\, l(u)}.$$

Moreover the line bundle on X corresponding to a point $\pi(l) \in \hat{X}$ $(l \in \overline{T})$ is then just $L(0, \alpha_l)$ where

$$\alpha_l(u) = e^{2\pi i \,\mathrm{Im}\, l(u)},\ u \in U.$$

There arises a small question of compatibility: we just constructed $\hat{X} = \overline{T}/U'$ and showed that $\hat{X} \simeq \mathrm{Pic}^0(X)$. But in §2, via the exact sequence

$$0 \longrightarrow \mathbf{Z} \longrightarrow \mathcal{O}_X \longrightarrow \mathcal{O}_X^* \longrightarrow 0,$$

we constructed an isomorphism

$$\mathrm{Pic}^0(X) \simeq H^1(X, \mathcal{O}_X)/H^1(X, \mathbf{Z})$$

and in §1, we found an isomorphism $H^1(X, \mathcal{O}_X) \simeq \overline{T}$. We would like to be sure that we have really found essentially the same description of $\mathrm{Pic}^0(X)$ twice. As we have just seen, our second description of $\mathrm{Pic}^0(X)$ rests on the map

$$\begin{array}{ccc} \overline{T} & \longrightarrow & \mathrm{Pic}^0(X) \\ l & \longmapsto & L(0, \alpha_l). \end{array}$$

Let us compute the composite map $\overline{T} \xrightarrow{\sim} H^1(\mathcal{O}_X) \xrightarrow{e^{2\pi i}} \mathrm{Pic}(X)$ which gave us the first description. This map is given by

$$\overline{T} \subset T \oplus \overline{T} \xrightarrow[f]{\sim} H^1(X, \mathbf{C}) \longrightarrow H^1(X, \mathcal{O}_X) \xrightarrow{e^{2\pi i}} \mathrm{Pic}(X).$$

Using group cohomology of U, we get a diagram

$$\begin{array}{ccccc} \mathrm{Hom}(U, \mathbf{C}) & \overset{\text{by def. of gp. coho.}}{=\!=} & H^1(U, \mathbf{C}) & \xrightarrow[e^{2\pi i}]{} & H^1(U, H^*) \\ \wr \| & & & & \\ \mathrm{Hom}_{\mathbf{R}}(V, \mathbf{C}) & & \wr \downarrow & & \wr \downarrow \\ \wr \downarrow & & & & \\ \overline{T} \subset T \oplus \overline{T} & \xrightarrow[f]{\sim} & H^1(X, \mathbf{C}) & \xrightarrow[e^{2\pi i}]{} & \mathrm{Pic}(X) \end{array}$$

where H^* = multiplicative group of non-zero holomorphic functions on V, and where the square on the left commutes according to the compactibilities verified in §1. Therefore, if $l \in \overline{T}$, the first description associates to l the U-co-cycle $u \to e^{2\pi i l(u)}$.

But

$$e^{2\pi i l(u)} = \frac{g(z+u)}{g(z)} \cdot e^{4\pi i \mathrm{Re}[l(u)]}$$

where $g(z) = e^{-2\pi i l(z)}$ is holomorphic in z. In other words, the first description rests on the map

$$\begin{array}{ccc} \overline{T} & \longrightarrow & \mathrm{Pic}^0(X) \\ l & \longmapsto & L(0, \alpha_l^*) \end{array}$$

$$\alpha_l^*(u) = e^{4\pi i \mathrm{Re}[l(u)]}.$$

So the two maps differ only by multiplication by $2i$ (experimental error!).

III

ALGEBRAIC THEORY VIA SCHEMES

10. The theorem of the Cube (II). In this chapter, we shall always mean by a scheme a scheme of finite type over an algebraically closed field k, and a point will always mean a closed point of the scheme.

We begin with the following seemingly innocuous generalization of Corollary 6 to the semicontinuity theorem.

PROPOSITION. *Let X be a complete variety, Y any scheme and L a line bundle on $X \times Y$. Then there exists a unique closed subscheme $Y_1 \hookrightarrow Y$ having the following properties:*

(a) *if L_1 is the restriction of L to $X \times Y_1$, there is a line bundle M_1 on Y_1 and an isomorphism $p_2^* M_1 \cong L_1$ on $X \times Y_1$;*

(b) *if $f : Z \to Y$ is any morphism such that there exists a line bundle K on Z and an isomorphism $p_2^*(K) \cong (1_X \times f)^*(L)$ on $X \times Z$, f can be factored as $Z \to Y_1 \hookrightarrow Y$.*

PROOF. The uniqueness is immediate, since if $Y_1 \hookrightarrow Y$ and $Y_1' \hookrightarrow Y$ are two closed subschemes of Y satisfying (a) and (b), each of these closed immersions can be factored through the other, and they must coincide.

Note next that if $p_2^* M_1 \cong L_1$, then $\underline{M}_1 \cong p_{2,*}(\underline{L}_1)$ (by the Künneth formula), hence to show that there is a line bundle M_1 such that $p_2^* M_1 \cong L_1$, it is equivalent to showing that $p_{2,*}(\underline{L}_1) = \mathfrak{M}_1$ is an invertible sheaf and the natural homomorphism $p_2^*(\mathfrak{M}_1) \to \underline{L}_1$ is an isomorphism.

In view of this, we are reduced to proving that there is an open covering $\{V_i\}$ of Y such that the proposition holds for $X \times V_i \to V_i$ and the restriction of L to $X \times V_i$. In fact, if we have done this, we obtain a closed subscheme $W_i \hookrightarrow V_i$ such that (a) and (b) are valid with Y replaced by V_i. Then clearly $W_i \cap (V_i \cap V_j)$ and $W_j \cap (V_i \cap V_j)$ are two closed subschemes of $V_i \cap V_j$ such that (a) and (b) hold with Y replaced by $V_i \cap V_j$, hence they are equal. Thus we obtain a closed subscheme Y_1 of Y such that $Y_1 \cap V_i = W_i$,

and (a) (because of our local reformulation) is clearly valid. As for (b), the local version of (b) implies that for each i, $f^{-1}(V_i) \to V_i$ factorizes through W_i hence $f^{-1}(V_i) \to Y$ factorizes through Y_1, and so $Z \xrightarrow{f} Y$ factorizes through Y_1.

Thus we may assume $Y = \operatorname{Spec} A$, and it suffices to find an open neighborhood of each point of Y in which the proposition is valid. By shrinking Y if necessary, we may assume that we have a free complex $0 \to A^{r_0} \xrightarrow{\phi} A^{r_1} \to \dots$ giving the direct images of L universally, as in §5. Let M be the cokernel of the transpose ${}^t\phi$ of $\phi: A^{r_1} \xrightarrow{{}^t\phi} A^{r_0} \to M \to 0$. Then for any A-algebra B, $B^{r_1} \xrightarrow{{}^t\phi_B} B^{r_0} \to M \otimes_A B \to 0$ is exact, and hence so is $0 \to \operatorname{Hom}_B(M \otimes_A B, B) \to B^{r_0} \xrightarrow{\phi_B} B^{r_1}$. This shows that for all $f: \operatorname{Spec} B \to \operatorname{Spec} A = Y$, $p_{2,*}((1_X \times f)^*(\underline{L})) \simeq \operatorname{Hom}_A(M, B)$. Now let F be the set of points $y \in Y$ such that the restriction $L_y = L \mid X \times \{y\}$ is trivial, so that F is a closed subset of Y by our earlier result (applied to Y_{red} and the restriction of L to $X \times Y_{\text{red}}$). If $Y' = Y - F$, the empty subscheme $Y_1 = \emptyset$ of Y' satisfies (a) and (b) with respect to Y'. Hence, it suffices to show that for any $y \in F$, y has an open neighborhood in which the proposition holds. If $y \in F$, $1 = \dim H^0(X \times \{y\}, \underline{L}_y) = \dim \operatorname{Hom}_A(M, A/\mathfrak{M}_y) = \dim_k \frac{M}{\mathfrak{M}_y M}$, so that by Nakayama's lemma, there is an element of M which generates M in an open neighborhood of y. Restricting ourselves to this neighborhood we may assume that $M \simeq A/\mathfrak{A}$, where $\mathfrak{A}$ is an ideal of A. Let Y_1' be the closed subscheme defined by $\mathfrak{A}$, L_1' the restriction of L to $X \times Y_1'$ and $\underline{L}_1'$ the associated sheaf. Then $p_{2,*}(\underline{L}_1')$ is the sheaf associated to $\operatorname{Hom}_A(A/\mathfrak{A}, A/\mathfrak{A}) \simeq A/\mathfrak{A}$ on Y_1', and is hence free of rank one. Consider the natural homomorphism $p_2^*(p_{2,*}(\underline{L}_1')) \xrightarrow{\lambda} L_1'$ on $X \times Y_1'$. Since both sides are locally free of rank one, this is an isomorphism, at a point $z \in X \times Y_1'$ if and only if the induced homomorphism of 'fibers'

$$[p_2^*(p_{2,*}(\underline{L}_1'))_z] \otimes_{\mathcal{O}_z} k \to [\underline{L}_{1z}'] \otimes_{\mathcal{O}_z} k$$

is surjective. Now, since $\operatorname{Hom}_A(A/\mathfrak{A}, A/\mathfrak{A}) \to \operatorname{Hom}_A(A/\mathfrak{A}, A/\mathfrak{M}_y) = H^0(X \times \{y\}, L|X \times \{y\})$ is surjective and $L|X \times \{y\}$ is trivial, λ is an isomorphism at all points of $X \times \{y\}$. On the other hand, the set Z of points on $X \times Y_1'$ where λ is not an isomorphism, being the union of the supports of $\ker \lambda$ and $\operatorname{coker} \lambda$, is closed and does not meet $X \times \{y\}$. Hence its projection into Y is a closed subset not containing y. By restricting ourselves to an affine open neighborhood of y not meeting this projection, we may assume that $M \simeq A/\mathfrak{A}$, and that if Y_1 is the closed subscheme defined by $\mathfrak{A}$, condition (a) is fulfilled on Y_1. We claim that (b) follows. In fact, since the condition that $f: Z \to Y$ factorize through Y_1 is local on Z, we may assume $Z = \operatorname{Spec} B$ affine, and B becomes an A-algebra via f. Further, we may assume K trivial on Z, so that $(1_X \times f)^*(\underline{L}) \simeq \mathcal{O}_{X \times Z}$ and $p_{2,*}(1_X \times f)^*(\underline{L}) \simeq p_{2,*}(\mathcal{O}_{X \times Z}) \simeq \mathcal{O}_Z$ (since X is a complete variety). Hence we have an isomorphism of B-modules $B \simeq \operatorname{Hom}_A(A/\mathfrak{A}, B)$, so that $\mathfrak{A}.B = 0$ and $A \to B$ factors through $A/\mathfrak{A}$. Thus f factors through Y_1, proving the proposition.

Under the assumptions of the proposition, we shall refer to the closed subscheme Y_1 of Y given by the proposition as the maximal closed subscheme of Y over which L is trivial.

We get the following strengthened version and direct proof of the theorem of the cube.

THEOREM. *Let X and Y be complete varieties, Z a connected scheme, and L a line bundle on $X \times Y \times Z$ whose restrictions to $\{x_0\} \times Y \times Z$, $X \times \{y_0\} \times Z$ and $X \times Y \times \{z_0\}$ are trivial for some $x_0 \in X, y_0 \in Y$, and $z_0 \in Z$. Then L is trivial.*

PROOF. Let Z' be the maximal closed subscheme of Z over which L is trivial, so that $Z' \neq \emptyset$ since $z_0 \in Z'$. We have to show that $Z' = Z$, and since Z is connected, it suffices to show that if a point belongs to Z', Z' contains an open neighborhood (considered as an open subscheme of Z) of that point. Let us denote this point again by z_0, by $\mathfrak{M}$ the maximal ideal of $\mathcal{O}_{Z,z_0}$ and by $I = I_{z_0}$ the

ideal defining Z' at z_0, so that $I \subset \mathfrak{M}$. We have to show that $I=(0)$. If not, since $\bigcap_{n>0} \mathfrak{M}^n = (0)$ by Krull's Theorem, we can find an integer $n > 0$ such that $\mathfrak{M}^n \supset I$, $\mathfrak{M}^{n+1} \not\supset I$, so that

$$[\mathfrak{M}^{n+1} + I/\mathfrak{M}^{n+1}] \subset [\mathfrak{M}^n/\mathfrak{M}^{n+1}]$$

is a non-zero k-vector space. Hence, if $\mathfrak{A}_1 = \mathfrak{M}^{n+1} + I$, we can find an ideal $\mathfrak{A}_2$ with $\mathfrak{A}_1 \supset \mathfrak{A}_2 \supset \mathfrak{M}^{n+1}$ and $\dim_k \frac{\mathfrak{A}_1}{\mathfrak{A}_2} = 1$. Hence $\mathfrak{A}_1 = \mathfrak{A}_2 + k.a$ for some $a \in \mathfrak{A}_1$ and $\mathfrak{A}_1 \supset I$ but $\mathfrak{A}_2 \not\supset I$. Let $\mathfrak{A}_0 = \mathfrak{M}$. Let z_i be the closed subschemes of Z consisting of the single point z_0, with structure sheaf $\mathcal{O}_{Z,z_0}/\mathfrak{A}_i$, so that:

$$\begin{array}{ccccc} & & Z' & & \\ & \cup & & \subset & \\ \{z_0\} = Z_0 & \subset & Z_1 & \subset & Z \\ & \cap & & \cup & \\ & & Z_2 & & \end{array}$$

Let $\underline{L}_i$ $(i=0,1,2)$ be the restriction to $X \times Y \times Z_i$ of the sheaf $\underline{L}$ of sections of L. Note that $\underline{L}_0, \underline{L}_1$ are trivial on $X \times Y \times Z_0$, $X \times Y \times Z_1$ respectively, since $Z_0, Z_1 \subset Z'$, so that we have isomorphisms $\underline{L}_i \simeq \mathcal{O}_{X \times Y \times Z_i}$ $(i=0,1)$. Further, since the structure sheaves of Z_0, Z_1 and Z_2 are related by the exact sequence

$$0 \longrightarrow \mathcal{O}_{Z_0} \xrightarrow{\text{mult. by } a} \mathcal{O}_{Z_2} \xrightarrow{\text{restr.}} \mathcal{O}_{Z_1} \longrightarrow 0,$$

we also have an exact sequence of sheaves on the topological space Z_0:

$$0 \longrightarrow \underline{L}_0 \xrightarrow{\text{mult. by } a} \underline{L}_2 \xrightarrow{\text{restr.}} \underline{L}_1 \longrightarrow 0.$$

Consider the section $s \in \Gamma(X \times Y \times Z_1, \underline{L}_1)$ equal to $\lambda(1)$ under the isomorphism λ: $\mathcal{O}_{X \times Y \times Z_1} \xrightarrow{\approx} \underline{L}_1$. The necessary and sufficient

condition that $\underline{L}_2$ be trivial is that s can be lifted to a section s' of $\underline{L}_2$. In fact, if we can do this, multiplication by s' is a homomorphism λ': $\mathcal{O}_{X \times Y \times Z_1} \to \underline{L}_2$ which reduced modulo the maximal ideal of any point ζ of $X \times Y \times \{z_0\}$ is an isomorphism $k \xrightarrow{\sim} \underline{L}_2 \otimes_{\mathcal{O}_\zeta} k$, hence λ' is an isomorphism (the sheaves being locally free). Conversely, if $\underline{L}_2$ is trivial, using the induced trivialization of $\underline{L}_1$, the map $\Gamma(\underline{L}_2) \to \Gamma(\underline{L}_1)$ becomes the map $\Gamma(\mathcal{O}_{Z_2}) \to \Gamma(\mathcal{O}_{Z_1})$, which is surjective. Now, fix an isomorphism $\underline{L}_0 \simeq \mathcal{O}_{X \times Y}$. The obstruction to lifting s to $\Gamma(\underline{L}_2)$ is then an element $\xi \in H^1(X \times Y, \mathcal{O}_{X \times Y})$. Since the restrictions of L to $X \times \{y_0\} \times Z$ and $\{x_0\} \times Y \times Z$, hence also to $X \times \{y_0\} \times Z_2$ and $\{x_0\} \times Y \times Z_2$, are trivial, the restrictions of s to $X \times \{y_0\} \times Z_1$ and $\{x_0\} \times Y \times Z_1$ can be lifted to $L \mid X \times \{y_0\} \times Z_2$ and $L \mid \{x_0\} \times Y \times Z_2$ respectively. This means that the image of ξ by the maps $H^1(X \times Y, \mathcal{O}_{X \times Y}) \to H^1(X, \mathcal{O}_X)$ and $H^1(X \times Y, \mathcal{O}_{X \times Y}) \to H^1(Y, \mathcal{O}_Y)$ induced by $x \longmapsto (x, y_0)$ and $y \longmapsto (x_0, y)$ are zero. But by the Künneth formula, these maps induce an isomorphism $H^1(X \times Y, \mathcal{O}_{X \times Y}) \simeq H^1(X, \mathcal{O}_X) \oplus H^1(Y, \mathcal{O}_Y)$. Therefore $\xi = 0$, and s can be lifted to $X \times Y \times Z_2$, and $\underline{L}_2$ is trivial. This is a contradiction, so Z' contains an open neighborhood of z_0.

11. **Basic Theory of Group Schemes.** We continue to work over a fixed algebraically closed field k, with schemes always of finite type over k, and with closed points only. $\underline{\text{Sch}}$ will denote the category of schemes of finite type over k.

One of the most basic tools in the theory of schemes is the concept of *S-valued points*: if X and S are schemes, an S-valued point of X is a morphism from S to X. The set of all such is denoted

$$\text{Hom}_k(S, X) \text{ or } \underline{X}(S).$$

If X is fixed, the map $S \longmapsto \underline{X}(S)$ is a contravariant functor:

$$\underline{X}\colon \underline{\text{Sch}}^0 \longrightarrow \underline{\text{Sets}}.$$

The importance of this functor is this: if X and Y are two schemes, then (a) a morphism $f\colon X \to Y$ defines a morphism from the functor

$\underline{X}$ to the functor $\underline{Y}$ (i.e. a map $\underline{X}(S) \xrightarrow{f(S)} \underline{Y}(S)$ for every S such that for every $g: S \to T$, the diagram

$$\begin{array}{ccc} \underline{X}(S) & \longleftarrow & \underline{X}(T) \\ {\scriptstyle f(S)}\downarrow & & \downarrow{\scriptstyle f(T)} \\ \underline{Y}(S) & \longleftarrow & \underline{Y}(T) \end{array}$$

commutes), and (b) conversely, a morphism from the functor $\underline{X}$ to the functor $\underline{Y}$ is defined by a unique morphism of schemes $f: X \to Y$. (a) and (b) are really tautologies holding for any category: the reader should prove them for himself if he has not seen them. This remark will turn out to be an excellent tool for constructing morphisms as we will see. Formally, (a) and (b) say that

$$X \longmapsto \underline{X}$$

is itself a fully faithful functor from the category $\underline{\text{Sch}}$ to the category Fun ($\underline{\text{Sch}}^0$, $\underline{\text{Sets}}$) of all contravariant functors from $\underline{\text{Sch}}$ to $\underline{\text{Sets}}$, hence $\underline{\text{Sch}}$ is equivalent to a full subcategory of Fun ($\underline{\text{Sch}}^0$, $\underline{\text{Sets}}$). Cf. Mumford [M 3], Ch. 2.

If $\underline{\text{Alg}}$ denotes the category of k-algebras of finite type, and $R \in \text{Obj } \underline{\text{Alg}}$, let us put $\underline{X}(R) = \underline{X}(\text{Spec } R)$. Then $\underline{X}$ defines a covariant functor from $\underline{\text{Alg}}$ to $\underline{\text{Sets}}$, which functor again we denote by the same symbol $\underline{X}$. The elements of $\underline{X}(R)$ are also referred to as R-valued points of X. If $\mathscr{C} = \text{Fun } (\underline{\text{Alg}}, \underline{\text{Sets}})$, it is once again an easy matter to show that $\text{Hom}_{\underline{\text{Sch}}}(X, Y) \xrightarrow{\sim} \text{Hom}_{\mathscr{C}}(\underline{X}, \underline{Y})$ is bijective, so that $\underline{\text{Sch}}$ can be identified with a full subcategory of $\mathscr{C}$.

DEFINITION. *A group scheme is a scheme G together with* (a) *a multiplication morphism $m: G \times G \to G$,* (b) *an identity point, i.e. a morphism e: Spec $k \to G$, and* (c) *an inverse morphism $i: G \to G$, such that the following axioms hold.*

(1) *(Associativity). The diagram*

$$\begin{array}{ccc} G \times G \times G & \xrightarrow{m \times 1_G} & G \times G \\ {\scriptstyle 1_G \times m}\downarrow & & \downarrow{\scriptstyle m} \\ G \times G & \xrightarrow{m} & G \end{array}$$

is commutative.

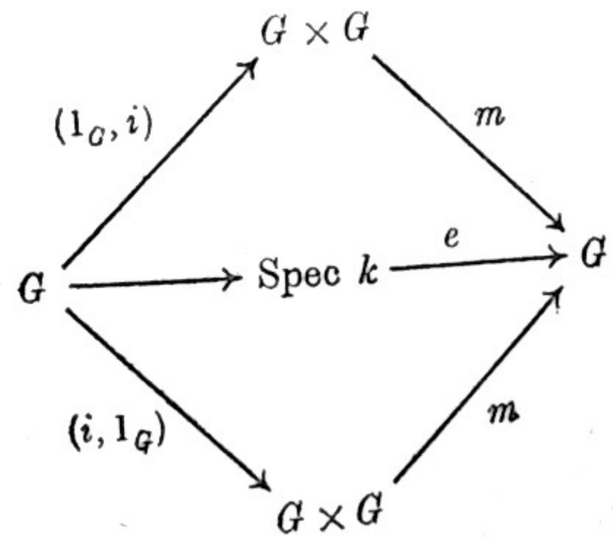
(2) *The diagram*

$$\begin{array}{ccc} G \times \text{Spec } k & \xrightarrow{1_G \times e} & G \times G \\ \wr\downarrow & & \downarrow{\scriptstyle m} \\ G & \xrightarrow{1_G} & G \end{array}$$

$$\begin{array}{ccc} \text{Spec } k \times G & \xrightarrow{e \times 1_G} & G \times G \\ \wr\uparrow & & \uparrow{\scriptstyle m} \\ G & \xrightarrow{1_G} & G \end{array}$$

is commutative.

(3) *The diagram*



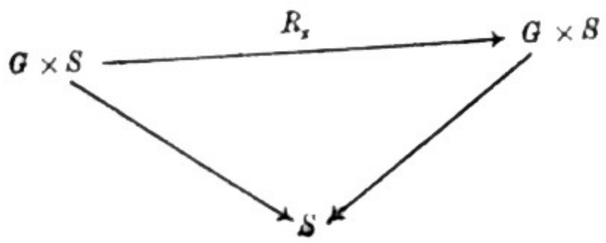
is commutative.

Now let G be a scheme, and let us interpret the conditions for giving a structure of group scheme to G in terms of the functor which it represents (either on Sch or on Alg). In view of our earlier remarks and the fact that products in Sch correspond to products of functors, m, i, and e can be interpreted respectively as maps $\underline{G}(S) \times \underline{G}(S) \to \underline{G}(S)$, $\underline{G}(S) \to \underline{G}(S)$, and as giving a distinguished element of $\underline{G}(S)$, functorially in S in the obvious sense. The conditions (1)-(3) then simply say that $\underline{G}(S)$ is a group for each S with m, i, and e defining the group law, inverse and identity element, and that for all morphisms $S' \to S$ of schemes, the induced map $\underline{G}(S) \to \underline{G}(S')$ is a group homomorphism. We thus see that to give a group scheme structure on a scheme G is *equivalent* to making the set of S-valued points of G into a group for every S, functorially in S. It would also be enough to make the set of R-valued points of G into a group, for every k-algebra R, functorially in R.

If x is an ordinary point of G, then the morphism

$$R_x\colon G \xrightarrow{\sim} G \times \{x\} \subset G \times G \xrightarrow{m} G$$

is an automorphism of G, called right-multiplication by x. More generally, if $x\colon S \to G$ is an S-valued point of G, x induces an automorphism R_x of $G \times S$ over S, which we can call right-multiplication by x. We use $m \circ (1_G \times x)\colon G \times S \to G$ and let $R_x = (m \circ (1_G \times x), p_2)$ so as to get a commutative diagram.



It is easy to check that with the group structure on $\underline{G}(S)$, we get $R_{x \cdot y} = R_y \circ R_x$. Interchanging the factors in $G \times G$, we can define left-multiplication L_x similarly.

Lie Algebras. Let X be a scheme, and Ω_X the sheaf of Kähler differentials on X over k. By a *vector field* on X we shall mean

a k-linear map of sheaves $D\colon \mathcal{O}_X \to \mathcal{O}_X$ such that the induced map $D\colon \mathcal{O}_X(U) \to \mathcal{O}_X(U)$ is a derivation over k, for every open set U. This is equivalent to saying that D factors:

$$\mathcal{O}_X \xrightarrow{d} \Omega_X \xrightarrow{f} \mathcal{O}_X ,$$

where f is an $\mathcal{O}_X$-linear homomorphism of sheaves.

By a tangent vector at $x \in X$, we mean a derivation $\mathcal{O}_{X,x} \to k$, or equivalently an element of $\operatorname{Hom}_{\mathcal{O}_{X,x}}(\Omega_{X,x}, k)$. Now, it is well known that if $\mathfrak{M}_x$ is the maximal ideal of $\mathcal{O}_{X,x}$ the natural map

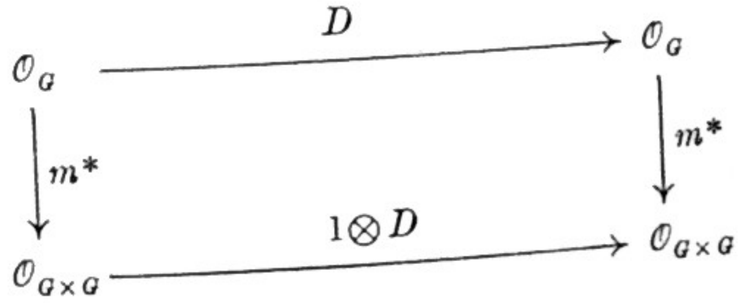
$$\frac{\mathfrak{M}_x}{\mathfrak{M}_x^2} \longrightarrow \Omega_{X,x} \otimes_{\mathcal{O}_{X,x}} k,$$

$$f \longmapsto df \otimes 1$$

is an isomorphism. Thus, a tangent vector is uniquely determined by giving a linear form on $\mathfrak{M}_x/\mathfrak{M}_x^2$. Clearly, a tangent field in a neighborhood of x determines a tangent vector at x (by composition of the derivation $\mathcal{O}_{X,x} \to \mathcal{O}_{X,x}$ and the evaluation map $\mathcal{O}_{X,x} \to k$), which we shall call the value of the vector field at x.

Let X and Y be two schemes, and D a vector field on X. If p_i ($i = 1,2$) denotes the i^{th} projection of $X \times Y$, we have a canonical isomorphism $p_1^*(\Omega_X) \oplus p_2^*(\Omega_Y) \xrightarrow{\sim} \Omega_{X \times Y}$, so that there is a unique vector field $D \otimes 1$ on $X \times Y$ such that when factored through $\Omega_{X \times Y}$, $D \otimes 1$ agrees on $p_1^*(\Omega_X)$ with D and it is zero on $p_2^*(\Omega_Y)$, i.e., $D \otimes 1(f \otimes g) = Df \otimes g$.

Now let G be a group scheme. A vector field D on G is said to be *left invariant* if the following diagram commutes:



the vertical maps being the natural ones induced by the multiplication morphism $G \times G \xrightarrow{m} G$.

PROPOSITION. *For any tangent vector t at e to G, there is a unique left invariant vector field on G having the value t at e.*

PROOF. First we interpret tangent vectors and vector fields in a slightly different way. Let Λ be the k-algebra $k[\epsilon]/(\epsilon^2)$ and η: $k[\epsilon]/(\epsilon^2) \to k$ the homomorphism with $\eta(\epsilon) = 0$. If A and B are k-algebras and B is an A-algebra, the k-derivations D of A in B are in one-one correspondence with algebra homomorphisms ϕ: $A \to \dfrac{B[\epsilon]}{(\epsilon^2)} \simeq B \otimes_k \Lambda$ such that $\phi(a) = a.1 +$ multiple of ϵ. This correspondence is given by $D \longleftrightarrow \phi$, $\phi(a) = a.1 + (Da).\epsilon$. Thus, we deduce that if X is a scheme and x a point of X, a tangent vector at x is a morphism $\operatorname{Spec} \Lambda \to X$ such that $\operatorname{Spec}(k) \hookrightarrow \operatorname{Spec} \Lambda \to X$ is the point x; and a vector field D on X is an automorphism over Λ:

$$\begin{array}{ccc} X \times \operatorname{Spec} \Lambda & \xrightarrow{\tilde{D}} & X \times \operatorname{Spec} \Lambda \\ & \searrow \quad \swarrow & \\ & \operatorname{Spec} \Lambda & \end{array}$$

which restricts to the identity 1_X: $X \to X$ when you look at the fibres over $\operatorname{Spec}(k) \hookrightarrow \operatorname{Spec}(\Lambda)$.

One then sees easily that a vector field D on a group scheme G is left invariant if and only if for the associated automorphism $\tilde{D}$, the diagram

$$\begin{array}{ccc} G \times G \times \operatorname{Spec} \Lambda & \xrightarrow{1_G \times \tilde{D}} & G \times G \times \operatorname{Spec} \Lambda \\ \downarrow{\scriptstyle m \times 1} & & \downarrow{\scriptstyle m \times 1} \\ G \times \operatorname{Spec} \Lambda & \xrightarrow{\tilde{D}} & G \times \operatorname{Spec} \Lambda \end{array} \qquad (*)$$

is commutative. If $D' = p_1 \circ \tilde{D}$: $G \times \operatorname{Spec} \Lambda \to G$, then in terms of S-valued points x, y of G and l of $\operatorname{Spec} \Lambda$, this diagram says:

$$D'(x.y, l) = x.D'(y, l).$$

This clearly holds if and only if $D'(x,l) = x.D'(e,l)$ for all x and l. In other words, if $\tilde{t}$ equals $p_1 \circ \tilde{D} \circ (e,1)$: $\operatorname{Spec} \Lambda \to G$ then we want $\tilde{D}$ to be right-multiplication by the Λ-valued point $\tilde{t}$ of G. Therefore given any Λ-valued point $\tilde{t}$ of G, we get a unique automorphism $\tilde{D}$ of $G \times \operatorname{Spec}(\Lambda)$ such that (*) commutes and $p_1 \circ \tilde{D} \circ (e,1) = \tilde{t}$. But this means exactly that D is left invariant and has value t at e.

Thus we get a canonical isomorphism of the k-vector space of left invariant vector fields on G and the tangent space at e to G. Now, given any two vector fields D_1, D_2 on a scheme X, considering them as endomorphisms of $\mathcal{O}_X$, we see that $D = [D_1, D_2] = D_1 D_2 - D_2 D_1$ is again a vector field on X, called the *Poisson bracket* of D_1 and D_2. Furthermore, if $\operatorname{char} k = p > 0$, D_1^p is again a vector field. If G is a group scheme, one verifies trivially that the Poisson bracket and p^{th} power operation take left invariant vector fields to left invariant vector fields.

DEFINITION. *The Lie algebra of a group scheme is the k-vector space of left invariant vector fields, together with the operation of Poisson bracket defined on it, as well as the p^{th} power operation if* $\operatorname{char} k = p > 0$.

We shall agree to denote the Lie algebra of G, H, G_1, ... etc. by $\mathfrak{g}$, $\mathfrak{h}$, $\mathfrak{g}_1$, ... etc. We have then:

(1) The map $\mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$, $(X, Y) \longmapsto [X, Y]$, is bilinear over k and the map $X \longmapsto X^p$ satisfies $(\lambda X)^p = \lambda^p X^p$.

(2) For $X \in \mathfrak{g}$, $[X, X] = 0$.

(3) For X, Y and $Z \in \mathfrak{g}$, we have
$$[X, [Y, Z]] + [Y, [Z, X]] + [Z, [X, Y]] = 0.$$

(4) If $\operatorname{char} k = p > 0$, there is a certain universal non-commutative polynomial F_p (depending only on p) in two variables such that

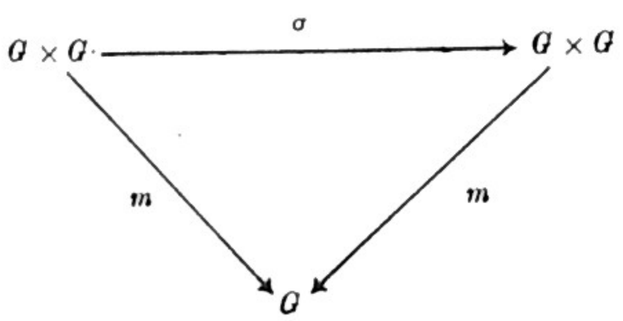
$$\text{ad}\,(X^p) = (\text{ad}\,X)^p,$$

$$(X+Y)^p = X^p + Y^p + F_p(\text{ad}\,X, \text{ad}\,Y)\,Y,$$

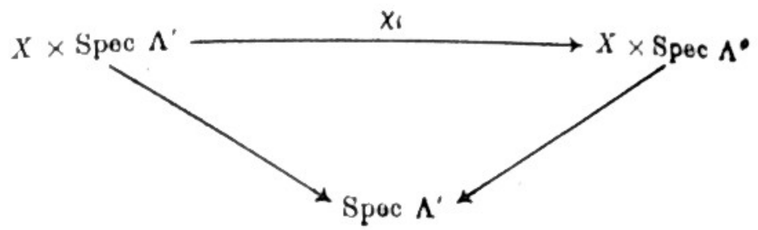
where ad X is the endomorphism of $\mathfrak{g}$ defined by $\text{ad}\,X(Y) = [X, Y]$.

For the actual expression of F_p, which is unimportant for our purposes, we refer to [J]. It is however uniquely determined by the condition that if A is an associative algebra over k and we define $[X, Y] = XY - YX$ and X^p to be the p^{th} power in A, A satisfies (4). Thus, F_p may be calculated by taking A to be a free associative algebra on two generators X and Y over k, and showing that $(X+Y)^p$ can be expanded as in (4) in A. Since we are mainly interested in the case when $\mathfrak{g}$ is "abelian", that is, when $[X, Y] = 0$ for $X, Y \in \mathfrak{g}$, it suffices for us to know that F_p has 'no constant term', that is, $F_p(0, 0) = 0$. Thus, in the abelian case, $X \to X^p$ is just a p-linear map (i.e. an additive homomorphism of $\mathfrak{g}$ into itself with $(\lambda X)^p = \lambda^p X^p$). In the case of the Lie algebra of an abelian variety, the p^{th} power map is called the Hasse-Witt map.

We remark that if G is commutative, that is, if the diagram



is commutative, where σ is the 'switch map' $\sigma = (p_2, p_1)$ then $\mathfrak{g}$ is abelian, that is, $[X, Y] = 0$ for all $X, Y \in \mathfrak{g}$. To prove this, we start with the following observation. Let D_i $(i = 1, 2)$ be vector fields on any scheme X, $D_3 = [D_2, D_1]$ and $\widetilde{D}_i$: $X \times \text{Spec}\,\Lambda \to X \times \text{Spec}\,\Lambda$ be the associated automorphisms, where $\Lambda = k[\epsilon]/(\epsilon^2)$. Put $\Lambda' = k[\epsilon, \epsilon']/(\epsilon^2, \epsilon'^2)$, and let $\sigma_i : \Lambda \to \Lambda'$ be the k-algebra homomorphisms defined by $\sigma_1(\epsilon) = \epsilon, \sigma_2(\epsilon) = \epsilon'$ and $\sigma_3(\epsilon) = \epsilon\epsilon'$. Then σ_i induces a morphism $\phi_i = \text{Spec}\,\sigma_i$: $\text{Spec}\,\Lambda' \to \text{Spec}\,\Lambda$ $(1 \leqslant i \leqslant 3)$, and we get automorphisms



by taking fibre products with Spec Λ' over Spec Λ via ϕ_i. One then checks easily (by taking X affine) that χ_3 is the commutator $[\chi_1, \chi_2] = \chi_1 \chi_2 \chi_1^{-1} \chi_2^{-1}$. Now suppose G is a group scheme, let t_i: $\text{Spec}\,\Lambda \to G$ $(i = 1, 2)$ tangent vectors at G, and let D_i be corresponding left invariant vector fields. Then $\widetilde{D}_i$ is just right-translation with respect to t_i, and if $t_i \circ \phi_i = T_i$: $\text{Spec}\,\Lambda' \to G$, then χ_i is right translation of $G \times \text{Spec}\,\Lambda'$ by the point $T_i \in \underline{G}(\Lambda')$. Hence $\chi_1 \chi_2 \chi_1^{-1} \chi_2^{-1}$ is right translation by $[T_1, T_2] \in \underline{G}(\Lambda')$. Since $\underline{G}(\Lambda')$ is a commutative group, it follows that $[T_1, T_2] = 0$, hence $\chi_1 \chi_2 \chi_1^{-1} \chi_2^{-1} = \chi_3 = \text{Identity}$, and $[D_1, D_2] = 0$.

THEOREM. *Any group scheme over a field k of characteristic 0 is smooth (and in particular reduced).*

PROOF. We show in fact that if X is any scheme over k of characteristic zero and x a point of X such that there exist vector fields $D_1, \ldots, D_n$ in a neighborhood of x with $n = \dim_k \dfrac{\mathfrak{M}_x}{\mathfrak{M}_x^2}$ inducing independent tangent vectors at x, then X is smooth at x. We can choose x_i $(1 \leqslant i \leqslant n)$ in $\mathfrak{M}_x$ such that they form a basis modulo $\mathfrak{M}_x^2$ of $\mathfrak{M}_x/\mathfrak{M}_x^2$ and $(D_i\, x_j)(x) = \delta_{ij}$. Since clearly $D_i(\mathfrak{M}_x^p) \subset \mathfrak{M}_x^{p-1}$, D_i extend to derivations of the completion $\hat{\mathcal{O}}_x$ of $\mathcal{O}_x$. Now, we have a unique continuous k-homomorphism α: $k[[t_1, \ldots, t_n]] \to \hat{\mathcal{O}}_x$ with $\alpha(t_i) = x_i$. On the other hand, define β: $\hat{\mathcal{O}}_x \to k[[t_1, \ldots, t_n]]$ by putting

$$\beta(f) = \sum_{\substack{\nu = (\nu_1, \ldots, \nu_n) \\ \nu_i \geqslant 0}} \frac{D^\nu f}{\nu!}(x).t^\nu$$

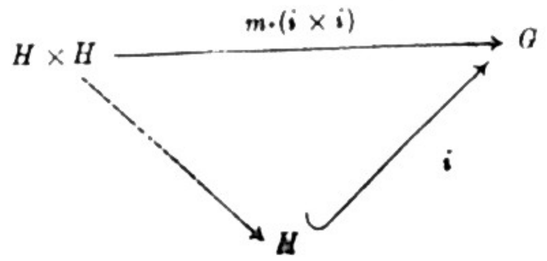
where $D^\nu f = D_1^{\nu_1} \ldots D_n^{\nu_n} f$, $\nu! = \nu_1! \ldots \nu_n!$ and $t^\nu = t_1^{\nu_1} \ldots t_n^{\nu_n}$. By Leibniz's formula and induction on n, one checks trivially that β is again a continuous k-homomorphism of local rings. Now,

α is surjective since its image contains a set of generators of $\mathfrak{M}_x$ and $k[[t_1, \dots, t_n]]$ is complete. On the other hand, $\beta(x_i) \equiv t_i \pmod{(t_1, \dots, t_n)^2}$ so that $\beta(x_i)$ generate the maximal ideal of $k[[t_1, \dots, t_n]]$, and β is also surjective. Hence so is $\beta \circ \alpha$, so that $\beta \circ \alpha$ is an automorphism of $k[[t_1, \dots, t_n]]$. Hence α is also injective, hence an isomorphism. Hence $\hat{\mathcal{O}}_x$ and $\mathcal{O}_x$ are regular, and X is smooth at x.

In positive characteristic, we will soon have plenty of examples of non-reduced group schemes.

SUBGROUP SCHEMES, KERNELS, QUOTIENTS.

Let G be a group scheme, and H a closed subscheme. We say that H is a *subgroup scheme* if, denoting by $i: H \hookrightarrow G$ the closed immersion, $m \circ (i \times i): H \times H \to G$ factors through H:



This is equivalent to saying that for every $S \in \text{Obj Sch}$, $\underline{H}(S)$ is a subgroup of $\underline{G}(S)$. Clearly H then becomes a group scheme in its own right, and $i: H \to G$ a homomorphism of group schemes (defined in an obvious way).

To any group scheme G over k of characteristic $p > 0$, one can associate in a natural way an increasing sequence G_n of closed subschemes ($n \geq 0$), all having support at the identity element of G, as follows. Let $\mathcal{O} = \mathcal{O}_e$ be the local ring at the identity to G, $\mathfrak{M}$ its maximal ideal, and $\mathfrak{M}^{(p^n)}$ the ideal generated by $\{x^{p^n} | x \in \mathfrak{M}\}$. Put $G_n = \text{Spec}\,[\mathcal{O}/\mathfrak{M}^{(p^n)}]$, so that G_n is a closed subscheme of G with support at e. Let $\mathcal{O}' = \mathcal{O}_{(e,e),G\times G}$ be the local ring of (e,e) on $G \times G$, so that $\mathcal{O}'$ is the localization of $\mathcal{O} \otimes_k \mathcal{O}$ with respect to the maximal ideal $\mathfrak{M} \otimes \mathcal{O} + \mathcal{O} \otimes \mathfrak{M}$. The multiplication map m induces a local homomorphism of rings $m^*: \mathcal{O} \to \mathcal{O}'$, so that for $f \in \mathfrak{M}$, $m^*(f) = g/h$,

$g \in \mathfrak{M} \otimes \mathcal{O} + \mathcal{O} \otimes \mathfrak{M}$, h a unit in $\mathcal{O}'$; hence $m^*(f^{p^n}) \in [\mathfrak{M}^{(p^n)} \otimes \mathcal{O} + \mathcal{O} \otimes \mathfrak{M}^{(p^n)}]\cdot \mathcal{O}'$. This proves that the composite $G_n \times G_n \to G \times G \xrightarrow{m} G$ factorizes through the subscheme G_n, proving that G_n is a subgroup scheme. One has evidently $\text{Lie}\,(G_n) = \text{Lie}\,G$ for $n > 1$.

EXAMPLES. (1) In any characteristic, define $\mathbf{G}_a$, the additive group over k, as $\text{Spec}\,k[T] = \mathbf{A}^1$, the group law $\mathbf{G}_a \times \mathbf{G}_a \to \mathbf{G}_a$ being defined by addition, or equivalently, by the homomorphism $m^*: k[T] \to k[T] \otimes k[T]$, $m^*(T) = T \otimes 1 + 1 \otimes T$. The group of S-valued points $\underline{\mathbf{G}}_a(S)$ is just the group $\Gamma(S, \mathcal{O}_S)$.

If $\text{char}\,k = p > 0$, we also write α_{p^n} for the subgroup scheme $(\mathbf{G}_a)_n$, that is $\alpha_{p^n} = \text{Spec}\left[\frac{k[T]}{(T^{p^n})}\right]$. We have $\text{Lie}\,(\mathbf{G}_a) = \text{Lie}\,(\alpha_{p^n}) = k.\partial/\partial T$, $n \geq 1$, and $\underline{\alpha}_{p^n}(S) = \{f \in \Gamma(S, \mathcal{O}_S) \,|\, f^{p^n} = 0\}$.

(2) In any characteristic, define $\mathbf{G}_m$ to be the multiplicative group over k, coinciding as a scheme with $\mathbf{A}^1 - \{0\}$, the group law being multiplication. Writing $\mathbf{G}_m = \text{Spec}\,k[T, 1/T]$, the homomorphism $m^*: k[T, 1/T] \to k[T, 1/T] \otimes_k k[T, 1/T]$ is given by $m^*(T) = T \otimes T$. The group of S-valued points of $\mathbf{G}_m$ is the group of units $\Gamma(S, \mathcal{O}_S^*)$.

If characteristic $k = p > 0$ we shall put $\mu_{p^n} = (\mathbf{G}_m)_n = \text{Spec}\,k[T, T^{-1}]/((T-1)^{p^n}) = \text{Spec}\,k[T]/(T^{p^n} - 1)$. We have $\text{Lie}\,\mathbf{G}_m = \text{Lie}\,\mu_{p^n} = k.T\,\partial/\partial T$ ($n \geq 1$), and $\underline{\mu}_{p^n}(S) = \{f \in \Gamma(S, \mathcal{O}_S^*) \,|\, f^{p^n} = 1\}$.

Now, let G and H be group schemes and $f: G \to H$ a homomorphism of group schemes. The fiber $f^{-1}(e_H) = G \times_H \{e_H\}$ over the closed point e_H of H which is the identity element of H is a closed subscheme K of G. By definition, for any S-valued point of G, $\phi: S \to G$, ϕ factorizes through K if and only if $f \circ \phi$ factorizes through $e_H: \text{Spec}\,k \to H$, or in other words, $\underline{K}(S)$ is the kernel of $\underline{G}(S) \to \underline{H}(S)$. Therefore K is a subgroup scheme of G.

As an example, consider the homomorphism $\mathbf{G}_m \to \mathbf{G}_m$ defined by $X \longmapsto X^n$. The kernel is denoted by μ_n. For $(n, p) = 1$, μ_n is just

a discrete group (i.e. reduced and finite group) isomorphic to the n^{th} roots of unity in k^*. On the other hand, it follows from definitions that μ_{p^n} is the same group defined earlier.

Next, suppose G and H are group schemes, and $\phi : H \to G$ a homomorphism. A pair $(G/H, \eta)$, where G/H is a scheme and $\eta : G \to G/H$ is a morphism, is said to be a *quotient* of G by H, if it is universal for all pairs (S,f) where S is a scheme, and $f : G \to S$ a morphism such that the following diagram commutes:

$$\begin{array}{ccc} H \times G & \xrightarrow{m \circ (\phi \times 1)} & G \\ \downarrow{\scriptstyle p_1} & & \downarrow \\ G & \xrightarrow{f} & S\,. \end{array}$$

It can be shown that quotients exist, that f is always flat and surjective, and further that when H is a normal subgroup scheme in G (i.e. $\underline{H}(S)$ is a normal subgroup of $\underline{G}(S)$ for all S), G/H inherits a unique structure of group scheme such that $\eta : G \to G/H$ is a homomorphism and has kernel precisely H. We will not need the result in this generality, but only in the special case when H is a finite group scheme. We will consider this in §12.

LEFT-INVARIANT DIFFERENTIAL OPERATORS.

We want to study the algebra of maps $\mathcal{O}_G \to \mathcal{O}_G$ generated by left-invariant derivations. We first introduce the *hyperalgebra* $\mathbf{H}$ of G :

$$\mathbf{H}_x = \mathrm{Hom}_{\mathrm{cont}}(\mathcal{O}_{x,G}, k)$$

$$\mathbf{H} = \bigoplus_{x \in G} \mathbf{H}_x$$

where $\mathrm{Hom}_{\mathrm{cont}}$ means the maps $L : \mathcal{O}_x \to k$ which are continuous in the sense that $L(\mathfrak{M}_x^{N+1}) = (0)$ for some N. Alternately,

$$\mathbf{H} = \varinjlim_{\substack{\text{0-dim-subschemes} \\ Z \subset G}} \Gamma(\mathcal{O}_Z)^*$$

where W^* means the k-vector space dual to a vector space W. If $L \in \mathbf{H}$ lies in the subspace $\Gamma(\mathcal{O}_Z)^*$, we will say that L is supported by Z. This definition makes it clear that $\mathbf{H}$ is an algebro-geometric analog of the space of distributions on a Lie group supported on a finite set. $\mathbf{H}$ has a lot of structure.

(1) We get an associative and distributive convolution product

$$* : \mathbf{H} \otimes \mathbf{H} \longrightarrow \mathbf{H}$$

by defining

$$(\S) \qquad L_1 * L_2(f) = L_1 \otimes L_2(m^* f).$$

More precisely, if L_i is supported by Z_i, $i = 1, 2$, and if $Z_3 \subset G$ is a finite subscheme such that the group law m factors :

$$\begin{array}{ccc} Z_1 \times Z_2 & \dashrightarrow & Z_3 \\ \cap & & \cap \\ G \times G & \xrightarrow{m} & G \end{array}$$

then $L_1 * L_2$ is to be supported by Z_3 and the equation (§) is to be interpreted with $f \in \Gamma(\mathcal{O}_{Z_3})$ and with m as the restriction of m to $Z_1 \times Z_2$.

(2) Evaluation at any point $x \in G$ is a continuous linear map $\delta_x : \mathcal{O}_x \to k$ hence an element $\delta_x \in \mathbf{H}$ supported by the point x with reduced structure. δ_e is a two-sided identity for convolution:

$$\delta_e * L = L * \delta_e = L.$$

Moreover, evaluation of elements $L \in \mathbf{H}$ at the function $1 \in \Gamma(\mathcal{O}_G)$ induces an augmentation

$$\epsilon : \mathbf{H} \longrightarrow k.$$

Note that if G is finite and reduced, the δ_x's are a basis of $\mathbf{H}$ over k, and since $\delta_x * \delta_y = \delta_{xy}$, $\mathbf{H}$ is nothing but the group algebra $k[G]$ of G.

(3) The ordinary product of functions $\mathcal{O}_x \otimes \mathcal{O}_x \to \mathcal{O}_x$ induces a co-product

$$s: \mathbf{H} \longrightarrow \mathbf{H} \otimes_k \mathbf{H}.$$

This satisfies many identities, which we will consider later in §14 for finite commutative group schemes G.

The interesting thing is that the elements $L \in \mathbf{H}$ extend uniquely to left-invariant operators $D_L : \mathcal{O}_G \to \mathcal{O}_G$ such that, roughly, $(D_L f)(e) = L(f)$. These operators D_L are combinations of differential operators (which for every open set $U \subset G$, map $\mathcal{O}_G(U)$ to $\mathcal{O}_G(U)$) and translation operators $f \longmapsto f'$, $f'(x) = f(xa)$, (which map $\mathcal{O}_G(U)$ to $\mathcal{O}_G(U.a^{-1})$). We need some definitions.

DEFINITION. *A differential operator D on a scheme X is a k-linear endomorphism of the structure sheaf $\mathcal{O}_X$ such that there is an integer $N \geqslant 0$ having the property that if $f \in \mathfrak{M}_x^{N+1}$, some $x \in X$, then $Df(x) = 0$. The least such N is called the order of D.*

For example, the differential operators of order 0 are multiplications by functions, and those of order 1 are the sums of derivations plus multiplications by f's. Now say $L \in \mathbf{H}$ is supported by

$$Z = \bigcup_{i=1}^{n} \operatorname{Spec}(\mathcal{O}_{a_i}/\mathfrak{M}_{a_i}^{d_i}).$$

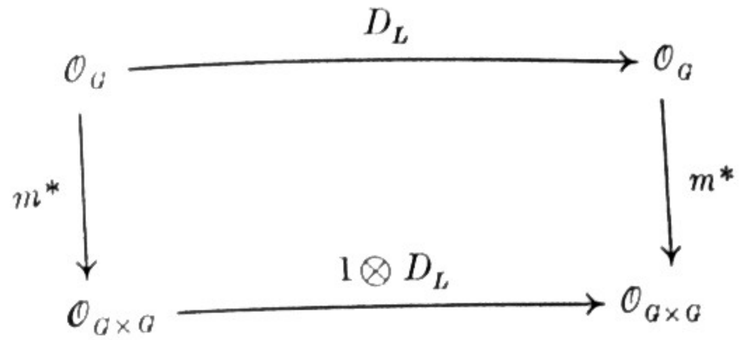
We then define an operator $D_L : \mathcal{O}_G \to \mathcal{O}_G$ which consists of a set of maps

$$D_L : \mathcal{O}_G(U) \longrightarrow \mathcal{O}_G(V)$$

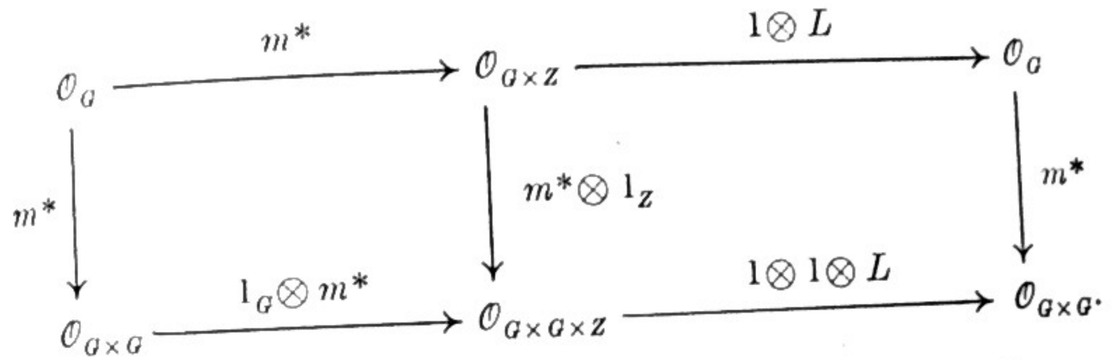
whenever $V.a_i \subset U$, $1 \leqslant i \leqslant n$, compatible with restrictions. We define D_L to be the composition:

$$\mathcal{O}_G \xrightarrow{m^*} \mathcal{O}_{G\times G} \xrightarrow{\text{res}} \mathcal{O}_{G\times Z} \xrightarrow{1\otimes L} \mathcal{O}_G.$$

It is easy to see that D_L is a sum of operators $D_{L,i}$ which are given by differential operators of order $< d_i$, followed by right translation by a_i. In particular, if $L \in \mathbf{H}_e$, then D_L is a differential operator. Moreover, D_L is left-invariant, i.e. the diagram



commutes. In fact, substituting the definition of D_L, this diagram becomes the outer rectangle of



The left-square commutes by associativity of the group law m, while the right square obviously commutes.

It follows immediately from the definition that if $f \in \mathcal{O}_G(U)$, and $a_i \in U$, $1 \leqslant i \leqslant n$, then $D_L f$ is defined at e and $D_L f(e) = L(f)$. The correspondence $L \longmapsto D_L$ generalizes the isomorphism $T_{e,G} \simeq$ {left-invariant derivations} used in defining the Lie algebra of G. In fact, the tangent space $T_{e,G}$ can be naturally identified with a subspace of $\mathbf{H}$:

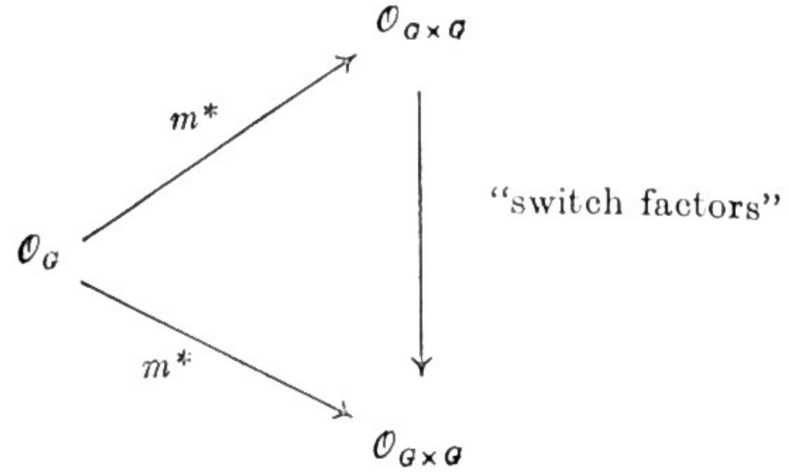
$$T_{e,G} \simeq \{L : \mathcal{O}_{e,G} \to k \mid L(1) = 0,\ L(\mathfrak{M}_e^2) = (0)\} \subset \mathbf{H},$$

and if $L \in T_{e,G}$, then D_L is the unique left-invariant derivation with value L at e. An important fact is that convolution of L's goes over to composition of operators:

$$(*) \qquad D_{L_1 * L_2} = D_{L_1} \circ D_{L_2}.$$

The proof is straightforward and is left to the reader. In particular, (*) shows that the Poisson bracket of left-invariant derivations can be interpreted by a commutator with respect to convolution product in $\mathbf{H}$ and that the p^{th} power on left-invariant

derivations can be interpreted as p^{th} power in $\mathbf{H}$. Note that if G is commutative, then $m^*: \mathcal{O}_G \to \mathcal{O}_{G\times G}$ is co-commutative, i.e.



commutes, and therefore convolution product in $\mathbf{H}$ will be commutative too.

This gives us a second proof that if G is commutative, then the bracket on its Lie algebra is zero.

To illustrate hyperalgebras, look at the simplest cases $G = \mu_p$ and $G = \alpha_p$. Writing

$$\mu_p = \operatorname{Spec} k[X]/(X^p - 1)$$
$$\alpha_p = \operatorname{Spec} k[X]/(X^p),$$

then in the first case all left-invariant differential operators are given by

$$f \longmapsto a_0 f + a_1 X \frac{df}{dX} + \ldots + a_{p-1} \cdot \left(X \frac{d}{dX}\right)^{p-1} f$$

and in the second case by

$$f \longmapsto a_0 f + a_1 \frac{df}{dX} + \ldots + a_{p-1} \frac{d^{p-1} f}{dX^p}.$$

Thus $\mathbf{H} \simeq k[D]/(D^p - D)$ or $\simeq k[D]/(D^p)$, where $D = X \dfrac{d}{dX}$ or $= \dfrac{d}{dX}$.

12. Quotients by Finite Group Schemes. An *action* of a group scheme G on a scheme X is a morphism:

$$\mu: G \times X \to X$$

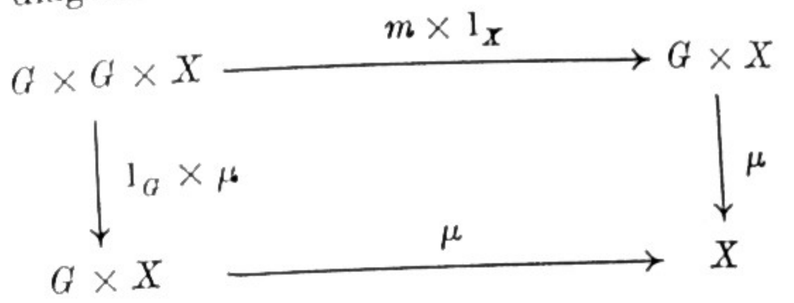
such that

(i) the composite

$$X \simeq \operatorname{Spec}(k) \times X \xrightarrow{e \times 1_X} G \times X \xrightarrow{\mu} X$$

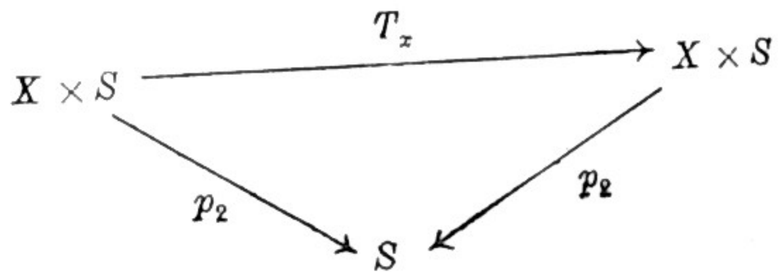
is the identity;

(ii) the diagram



is commutative.

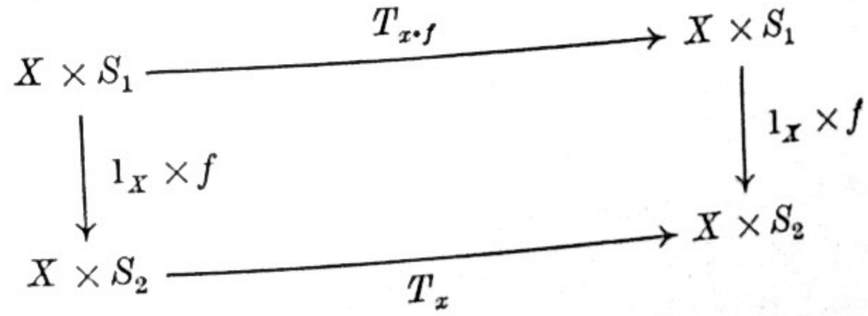
(Here, as usual, e is the identity and m is multiplication.) This is equivalent to saying that $\underline{G}(S)$ acts on $\underline{X}(S)$ for every scheme S (or even every affine S), functorially in S. It is also equivalent to saying that for every S-valued point $x \in \underline{G}(S)$, we are given an automorphism over S:



such that

(i) if $x, y \in \underline{G}(S)$, then $T_x \circ T_y = T_{x \cdot y}$;

(ii) if $f: S_1 \to S_2$ is any morphism, $x: S_2 \to G$ is an S_2-valued point, so $x \circ f: S_1 \to G$ is an S_1-valued point, then



commutes.

Explicitly, the T_x's are induced by μ via the formula $T_x = (\mu \circ \sigma \circ (1_X \times x), p_2)$ where $\sigma: X \times G \to G \times X$ is the switch morphism; and conversely, if we let $S = G$ and take x to be the G-valued point $1_G: G \to G$ of G, then $p_1 \circ T_x: X \times G \to X$ is just μ (except for the factors being reversed).

A morphism $f: X \to Y$ is said to be *G-invariant* if the diagram

$$\begin{array}{ccc} G \times X & \xrightarrow{\mu} & X \\ {\scriptstyle p_2}\downarrow & & \downarrow{\scriptstyle f} \\ X & \xrightarrow{f} & Y \end{array}$$

is commutative, i.e. in terms of S-valued points g and x of G and X, $f(\mu(g, x)) = f(x)$. In particular, taking $Y = \mathbf{A}^1$, we get the notion of a G-invariant function. We say that the action of G on X is *free* if the morphism

$$(\mu, p_2): G \times X \longrightarrow X \times X$$

is a closed immersion.

The action of a group G on a scheme X has a differential-geometric as well as a set-theoretic aspect. Let $\mathbf{H}_e$ be the part of the hyperalgebra of G with supports at e, and let $L \in \mathbf{H}_e$. Then L defines a differential operator D_L on X via

$$\mathcal{O}_X \xrightarrow{\mu^*} \mathcal{O}_{G \times X} \xrightarrow{L \otimes 1} \mathcal{O}_{\{e\} \times X} \approx \mathcal{O}_X.$$

It is easy to check that (a) $D_{L_1 * L_2} = D_{L_2} \circ D_{L_1}$, (b) D_{δ_e} is the identity, and (c) if $L \in T_{e,G} \subset \mathbf{H}_e$, then D_L is a differential operator of order 1, i.e. a derivation from $\mathcal{O}_X$ to $\mathcal{O}_X$. In particular, the Lie algebra of G is represented by derivations of $\mathcal{O}_X$.

Let $\mathcal{F}$ be a coherent sheaf on X. A *lift* of the action μ to $\mathcal{F}$ is by definition an isomorphism $\lambda: p_2^*(\mathcal{F}) \xrightarrow{\sim} \mu^*(\mathcal{F})$ of sheaves on $G \times X$ such that the diagram of sheaves on $G \times G \times X$,

$$\begin{array}{ccc} p_3^*(\mathcal{F}) & \xrightarrow{(p_2, p_3)^*(\lambda)} & \xi^*(\mathcal{F}) \\ & {\scriptstyle (m \times 1_X)^*(\lambda)} \searrow \quad \swarrow {\scriptstyle (1_G \times \mu)^*(\lambda)} & \\ & \eta^*(\mathcal{F}) & \end{array}$$

where $\xi = \mu \circ (p_2, p_3)$, $\eta = \mu \circ (m \times 1_X) = \mu \circ (1_G \times \mu)$, and p_i is the ith projection of $G \times G \times X$, is commutative.

A more manipulable way of defining a lift of an action μ to $\mathcal{F}$ is to require, for every S-valued point f of G, an automorphism λ_f of the sheaf $\mathcal{F} \otimes \mathcal{O}_S$ on $X \times S$ covering the automorphism μ_f of $X \times S$

$$\begin{array}{ccc} \mathcal{F} \otimes \mathcal{O}_S & \xrightarrow{\lambda_f} & \mathcal{F} \otimes \mathcal{O}_S \\ X \times S & \xrightarrow[\mu_f]{} & X \times S \end{array}$$

such that (1) the λ_f's are functorial in f, and (2) $\lambda_{f \cdot g} = \lambda_f \circ \lambda_g$.

Having stated these definitions, let us generalize the principal results of §7 on quotients by finite groups to quotients by finite group schemes. The following theorem is proved analogously to the first proposition of §7, so that we content ourselves with stating the necessary modifications.

THEOREM 1. (A) *Let G be a finite group scheme acting on a scheme X such that the orbit of any point is contained in an affine open subset of X. Then there is a pair (Y, π), where Y is a scheme and $\pi: X \to Y$ a morphism, satisfying the following conditions:*

(i) *as a topological space, (Y, π) is the quotient of X for the action of the underlying finite group;*

(ii) *the morphism $\pi: X \to Y$ is G-invariant, and if $\pi_*(\mathcal{O}_X)^G$ denotes the subsheaf of $\pi_*(\mathcal{O}_X)$ of G-invariant functions, the natural homomorphism $\mathcal{O}_Y \to \pi_*(\mathcal{O}_X)^G$ is an isomorphism.*

The pair (Y, π) is uniquely determined up to isomorphism by these conditions. The morphism π is finite and surjective. Y will be denoted X/G, and it has the functorial property: $\forall$ G-invariant morphisms $f: X \to Z$, $\exists$ a unique morphism $g: Y \to Z$ such that $f = g \circ \pi$.

(B) *Suppose further that the action of G is free and $G = \mathrm{Spec}(R)$, $n = \dim_k R$. Then π is a flat morphism of degree n, i.e. $\pi_*(\mathcal{O}_X)$ is a locally free $\mathcal{O}_Y$-module of rank n, and the subscheme of $X \times X$ defined by the closed immersion*

$$(\mu, p_2) : G \times X \longrightarrow X \times X$$

is equal to the subscheme $X \times_Y X \subset X \times X$. Finally, if $\mathcal{F}$ is a coherent $\mathcal{O}_Y$-module, $\pi^*\mathcal{F}$ has a naturally defined G-action lifting that on X, and

$$\mathcal{F} \longmapsto \pi^*\mathcal{F}$$

is an equivalence of the category of coherent $\mathcal{O}_Y$-modules (resp. locally free $\mathcal{O}_Y$-modules of finite rank) and the category of coherent $\mathcal{O}_X$-modules with G-action (resp. locally free $\mathcal{O}_X$-modules of finite rank with G-action).

Proof of (A). As before we are reduced to the case when $X = \mathrm{Spec}\ A$ is affine. Let R be the ring of G, $\epsilon: R \to k$ the evaluation map at e, $m^*: R \to R \otimes_k R$ and $\mu^* : A \to R \otimes_k A$ the homomorphisms of k-algebras induced by m and μ. Let $B = A^G = \{a \in A \mid \mu^*(a) = 1 \otimes a\}$ be the algebra of G-invariants in A. Let $\mathrm{Nm}_A : R \otimes_k A \to A$ be the norm mapping (defined since $R \otimes_k A$ is free of finite rank over A), so that Nm is a homogeneous polynomial function over A of degree $n = \dim_k(R)$ which is multiplicative. Define $N: A \to A$ by putting $N(\alpha) = \mathrm{Nm}(\mu^*(\alpha))$, so that N is again multiplicative and k-homogeneous of degree n. We assert that $N(A) \subset B$.

To prove this, we have to show that for any $\alpha \in A$, $\mu^*(N(\alpha)) = 1 \otimes N\alpha$. For any k-algebra B, denote by Nm_B the norm mapping $R \otimes_k B \to B$. Define $\phi : A \to R \otimes_k A$ and $\psi : R \otimes_k R \otimes_k A \to R \otimes_k R \otimes_k A$ by setting

$$\phi(a) = 1 \otimes a,$$

$$\psi(\xi \otimes \eta \otimes a) = (m^*(\xi) \otimes 1)(1 \otimes \eta \otimes a).$$

Note that if $f : B \to C$ is a homomorphism of k-algebras, we have $\mathrm{Nm}_C \circ (1_R \otimes f) = f \circ \mathrm{Nm}_B$. We thus have

$$\begin{aligned}
\mu^* \circ N &= \mu^* \circ \mathrm{Nm}_A \circ \mu^* \\
&= \mathrm{Nm}_{R \otimes_k A} \circ (1_R \otimes \mu^*) \circ \mu^* \\
&= \mathrm{Nm}_{R \otimes_k A} \circ (m^* \otimes 1_A) \circ \mu^* \\
&= \mathrm{Nm}_{R \otimes_k A} \circ \psi \circ (1_R \otimes \phi) \circ \mu^*.
\end{aligned}$$

Now, if we consider $R \otimes_k R \otimes_k A$ as an $R \otimes_k A$ algebra via the homomorphism $R \otimes_k A \to R \otimes_k R \otimes_k A$ given by $\eta \otimes a \longmapsto 1 \otimes \eta \otimes a$, ψ is an automorphism of the $R \otimes_k A$ algebra $R \otimes_k R \otimes_k A$, so that $\mathrm{Nm}_{R \otimes_k A} \circ \psi = \mathrm{Nm}_{R \otimes_k A}$. Thus, we obtain

$$\begin{aligned}
\mu^* \circ N &= \mathrm{Nm}_{R \otimes_k A} \circ (1_R \otimes \phi) \circ \mu^* \\
&= \phi \circ \mathrm{Nm}_A \circ \mu^* \\
&= \phi \circ N.
\end{aligned}$$

This proves our assertion.

Now, G also acts on $X \times \mathbf{A}^1$, (by acting trivially on $\mathbf{A}^1$), so that $N: A[T] \to A[T]$ is also defined. For any $a \in A$, put $\chi_a(T) = N(T - a)$. Then $\chi_a(T) = T^n + s_1 T^{n-1} + \cdots + s_n$ is G-invariant, and is the characteristic polynomial of the endomorphism of the free A-module $R \otimes_k A$ defined by the element $\mu^*(a)$. Since $\epsilon \otimes 1: R \otimes_k A \to A$ is surjective and $(\epsilon \otimes 1)(\mu^*(a)) = a$, $\mu^*(a) - a$ defines the zero map on the quotient A of $R \otimes_k A$ (via $\epsilon \otimes 1$), hence $\det(\mu^*(a) - a) = \chi_a(a) = 0$. The equation $\chi_a(a) = 0$ shows that a is integrally dependent on B. Thus A is integral over B. Since A is finitely generated over k, A is also integral over a finitely generated subalgebra of B. Thus A and hence B is a finite module over this subalgebra, and so B is also finitely generated over k. Let $Y = \mathrm{Spec}\ B$ and let $\pi: X \to Y$ be the induced morphism. Then π is finite and surjective. Using the map N, one sees as before that π separates orbits, so that (i) holds. Further π is clearly G-invariant, so that we have an inclusion $\mathcal{O}_Y \subset \pi_*(\mathcal{O}_X)^G$, inducing isomorphism of global sections. On the other hand, $\pi_*(\mathcal{O}_X)^G$ is a coherent $\mathcal{O}_Y$-module, being the kernel

of the $\mathcal{O}_Y$-homomorphism $\lambda : \pi_*(\mathcal{O}_X) \to \pi_*(\mathcal{O}_X) \otimes_k R$, $\lambda(f) = \mu^*(f) - f \otimes 1$, and this shows that $\mathcal{O}_Y = \pi_*(\mathcal{O}_X)^G$. This proves (ii).

PROOF OF (B). For the construction of the G-action on $\pi^*(\mathcal{F})$, the basic fact is the following. If $X \xrightarrow{f} Y \xrightarrow{g} Z$ are morphisms and $\mathcal{F}$ a sheaf of $\mathcal{O}_Z$-modules, there is a natural isomorphism $\lambda_{f,g}(\mathcal{F}) : (g \circ f)^*(\mathcal{F}) \xrightarrow{\sim} f^*(g^*(\mathcal{F}))$, satisfying the following condition: if $X \xrightarrow{f} Y \xrightarrow{g} Z \xrightarrow{h} T$ are morphisms, the square

$$\begin{array}{ccc} f^*g^*h^*(\mathcal{F}) & \xrightarrow{f^*(\lambda_{g,h})} & f^*(h\circ g)^*(\mathcal{F}) \\ \downarrow{\scriptstyle \lambda_{f,g}(h^*(\mathcal{F}))} & & \downarrow{\scriptstyle \lambda_{f,h\circ g}} \\ (g\circ f)^*h^*(\mathcal{F}) & \xleftarrow{\lambda_{g\cdot f\circ h}} & (h\circ g\circ f)^*(\mathcal{F}) \end{array}$$

is commutative.

Returning to our special case, the equality of the two composites $G \times X \underset{p_2}{\overset{\mu}{\rightrightarrows}} X \xrightarrow{\pi} Y$ enables us (by means of λ) to define an isomorphism λ: $p_2^*(\mathfrak{g}) \to \mu^*(\mathfrak{g})$, $\mathfrak{g} = \pi^*(\mathcal{F})$, and one checks that this is an action, using the above remark.

On the other hand, let $\mathfrak{g}$ be a sheaf on X with a G-action covering the action on X. A section $\sigma \in \mathfrak{g}(X)$ is said to be G-invariant if $\lambda(p_2^*(\sigma)) = \mu^*(\sigma)$. Localizing, we have the notion of the subsheaf $\pi_*(\mathfrak{g})^G$ of G-invariants of $\pi_*(\mathfrak{g})$. This is clearly an $\mathcal{O}_Y$-module which is coherent, being the subsheaf of $\pi_*(\mathfrak{g})$ where two $\mathcal{O}_Y$-homomorphisms $\pi_*(\mathfrak{g}) \rightrightarrows \pi_*(\mathfrak{g} \otimes_k R)$ coincide. As before, we have evident natural transformations $S(\mathcal{F}) : \mathcal{F} \to \pi_*(\pi^*(\mathcal{F}))^G$ and $T(\mathfrak{g}) : \pi^*(\pi_*(\mathfrak{g})^G) \to \mathfrak{g}$, and it is again sufficient to show that (when the action is free) π is flat, $G \times X \xrightarrow{\sim} X \times_Y X$, and $T(\mathfrak{g})$ is an isomorphism for every G-sheaf $\mathfrak{g}$ on X (as in the proof of Proposition 2, §7). In view of these remarks, since all the definitions localize, we may assume $X = \operatorname{Spec} A$ affine. Recall that the freeness of the action means that the morphism

$$(\mu, p_2) : G \times X \longrightarrow X \times X$$

is a closed immersion. Since π is G-invariant, (μ, p_2) factors through a closed immersion of $G \times X$ into $X \times_Y X$. On the ring level, this means that the homomorphism

$$\lambda : A \otimes_B A \longrightarrow R \otimes_k A$$

$$\lambda(a_1 \otimes a_2) = \mu^*(a_1) \cdot (1 \otimes a_2)$$

is surjective. We have to show (a) that A is flat over $B = A^G$ and λ is injective, (b) if $\mathfrak{g}$ is a G-sheaf on X with $\mathfrak{g}(X) = M$, $A \otimes_B M^G \to M$ is an isomorphism, and (c) if M is projective over A, M^G is B-projective. Note however that (c) is an immediate consequence of (a) and (b). In fact, it suffices to show that M^G is B-flat, i.e. the functor $N \longmapsto N \otimes_{A^G} M^G$ is exact on the category of A^G-modules, and since A is faithfully flat over A^G, it suffices to show that $N \longmapsto (N \otimes_{A^G} M^G) \otimes_{A^G} A \simeq (N \otimes_{A^G} A) \otimes_A (A \otimes_{A^G} M^G) \simeq (N \otimes_{A^G} A) \otimes_A M$ is exact, and this holds in view of (a).

To prove (a), we may pass to the ring of quotients of A and B with respect to $S = B - \mathfrak{M}$, where $\mathfrak{M}$ is a maximal ideal of B, so that we may assume B local and A semilocal.

If we consider $A \otimes_B A$ and $R \otimes_k A$ as A-modules through their second factors, λ is a surjective A-homomorphism, so that $R \otimes_k A$ is generated by $\mu^*(A)$. Since A is semilocal and $\mu^*(A)$ generates the free module $R \otimes_k A$, one shows easily that there are $\{a_i\}$ $(1 < i < n = \dim_k R)$ such that $\mu^*(a_i)$ form a basis of $R \otimes_k A$ over A. Now suppose $a, \lambda_1, \ldots, \lambda_n \in A$. I claim:

$$\left[\mu^*(a) = \sum_{i=1}^{n} (1 \otimes \lambda_i) \cdot \mu^*(a_i) \right] \qquad (*)$$

$$\Longleftrightarrow \left[a = \sum \lambda_i a_i \text{ and } \lambda_1, \ldots, \lambda_n \in B \right].$$

The implication $\Leftarrow$ is obvious by applying μ^* and using the fact that $\mu^*(\lambda_i) = (1 \otimes \lambda_i)$ if $\lambda_i \in B$. To prove $\Rightarrow$, use the fact that $(1 \otimes \mu^*)(\mu^* a) = (m^* \otimes 1)(\mu^* a)$ in $R \otimes_k R \otimes_k A$, hence substituting the expansion of $\mu^* a$, we deduce that

$$\sum_1^n (1 \otimes \mu^* \lambda_i) \cdot (1 \otimes \mu^*)(\mu^* a_i) = \sum_1^n (1 \otimes 1 \otimes \lambda_i) \cdot (m^* \otimes 1)(\mu^* a_i)$$

$$= \sum_1^n (1 \otimes 1 \otimes \lambda_i) \cdot (1 \otimes \mu^*)(\mu^* a_i).$$

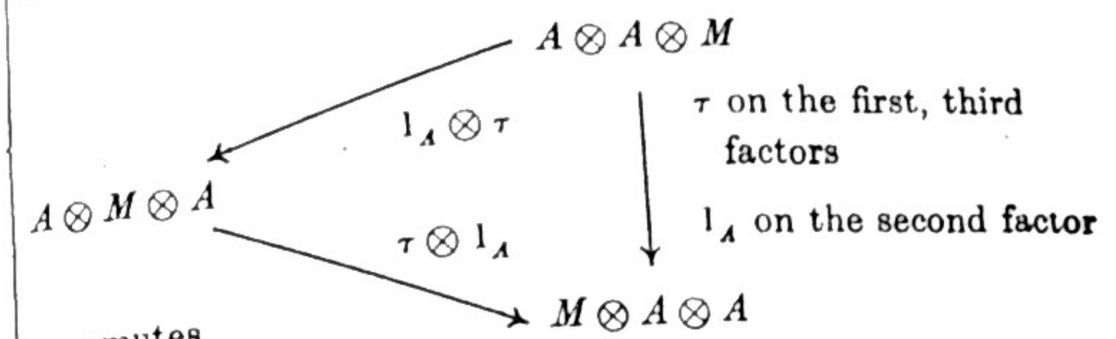
Since the $\mu^*(a_i)$ are linearly independent over A in $R \otimes_k A$, $(1 \otimes \mu^*)(\mu^* a_i)$ are linearly independent over $R \otimes_k A$ in $R \otimes_k R \otimes_k A$, the latter being considered as an algebra over the former via the last two factors. Hence the above equation yields that $1 \otimes \mu^* \lambda_i = 1 \otimes 1 \otimes \lambda_i$ i.e. $\lambda_i \in A^G = B$. Applying the homomorphism $\epsilon \otimes 1$ to the equation $\mu^*(a) = \Sigma(1 \otimes \lambda_i).\mu^*(a_i)$, we get that $a = \Sigma \lambda_i a_i$, as required. This proves (*). But (*) says that A is a free B-module with basis $a_1, \ldots, a_n$ and that the homomorphism $\lambda : A \otimes_B A \to R \otimes_k A$, regarded as a map of free A-modules via the second factor, takes the basis $a_i \otimes 1$ of the module on the left to the basis $\mu^*(a_i)$ of the module on the right. Therefore λ is an isomorphism.

We now prove (b). If $M = \mathfrak{g}(X)$ is the A-module corresponding to $\mathfrak{g}$, we first interpret the action of G on $\mathfrak{g}$ in terms of M. Firstly, $M \otimes_B A$ and $A \otimes_B M$ will be considered as $A \otimes_B A$-modules, where the first and second factors in $A \otimes_B A$ act on the first and second factors of the modules. It is easy to see that these are the two $A \otimes_B A$-modules obtained from the A-module M by tensor product with respect to the two homomorphisms $A \rightrightarrows A \otimes_B A$, $a \longmapsto a \otimes 1$ and $a \longmapsto 1 \otimes a$. In view of this, and the fact that $R \otimes_k A$ is naturally isomorphic to $A \otimes_B A$, it is easily checked that an action of G on $\mathfrak{g}$ amounts to an isomorphism of $A \otimes_B A$-modules :

$$\tau : A \otimes_B M \longrightarrow M \otimes_B A$$

such that

(α) if $M \otimes_B A \otimes_B A$, $A \otimes_B M \otimes_B A$, $A \otimes_B A \otimes_B M$ denote the usual $A \otimes_B A \otimes_B A$-modules, then the diagram:



commutes.

What is to be proven is that if N is the sub-B-module of M:

$$N = \{m \in M \mid \tau(1 \otimes m) = m \otimes 1\},$$

then the natural map $N \otimes_B A \to M$ is an isomorphism. We may rephrase the definition of N, and say that N is the kernel of the homomorphism of B-modules :

$$\phi : M \longrightarrow M \otimes_B A$$

$$\phi(m) = m \otimes 1 - \tau(1 \otimes m).$$

Since A is flat over B, it follows that $N \otimes_B A$ is the kernel of the homomorphism

$$\psi : M \otimes_B A \longrightarrow M \otimes_B A \otimes_B A$$

$$\psi(m \otimes a) = m \otimes 1 \otimes a - \tau(1 \otimes m) \otimes a.$$

In other words,

$$N \otimes_B A = \left\{ \sum m_i \otimes a_i \in M \otimes_B A \,\middle|\, \sum m_i \otimes 1 \otimes a_i = \sum \tau(1 \otimes m_i) \otimes a_i \right\}.$$

But the associative law (α), applied to the element $1 \otimes 1 \otimes m \in A \otimes A \otimes M$, says exactly that $\tau(1 \otimes m) \in M \otimes_B A$ has the property described in this equation. Therefore regarding $N \otimes_B A$ and $\tau(1 \otimes M)$ as two subsets of $M \otimes_B A$, we find $N \otimes_B A \supset \tau(1 \otimes M)$. Now both of them are modules over the subring $1 \otimes A \subset A \otimes_B A$. Moreover, $N \otimes_B A$ is generated over this ring by the elements $n \otimes 1$, $n \in N$, and since $\tau(1 \otimes n) = n \otimes 1$, these elements are in $\tau(1 \otimes M)$. Therefore $N \otimes_B A = \tau(1 \otimes M)$. But finally the maps

$$M \longrightarrow 1\otimes M \xrightarrow{\tau} \tau(1\otimes M)$$
$$m \longmapsto 1\otimes m$$

are isomorphisms, since A is faithfully flat over B, hence we obtain an isomorphism $N\otimes_B A \simeq M$. This is clearly the canonical map too, so (b) is proven.

DEFINITION: *A homomorphism $f: X \to Y$ of group schemes is an epimorphism if f is surjective and $f^*: \mathcal{O}_Y \to f_*\mathcal{O}_X$ is injective.*

COROLLARY 1. *Suppose X itself is a group scheme and G is a finite normal† subgroup scheme, acting on X by right-translation. Then X/G is again a group scheme, $\pi: X \to X/G$ is an epimorphism, and $G = \ker(\pi)$. Conversely, if $f: X \to Y$ is an epimorphism of group schemes, and if $G = \ker(f)$ is finite, then $Y \simeq X/G$.*

In other words, for every group scheme X we get a Galois-type correspondence between (a) normal finite subgroup schemes G, and (b) finite epimorphisms $\pi: X \to Y$. In fact, if the word "finite" is dropped from (a) and (b), the correspondence is still correct, but we will not prove this.

PROOF. First, say X is a group scheme and $G \subset X$ a finite normal subgroup. Let $m: X \times X \to X$ be the group law and consider the solid arrows in the diagram:

$$\begin{array}{ccc} X\times X & \xrightarrow{\ m\ } & X \\ \downarrow{\scriptstyle \pi\times\pi} & & \downarrow{\scriptstyle \pi} \\ X/G\times X/G & \dashrightarrow & X/G. \end{array}$$

Then $X/G \times X/G$ is the quotient of $X \times X$ by $G \times G$, and I claim that $\pi \circ m$ is a $G \times G$-invariant morphism. In fact, if x_1, x_2, g_1, g_2 are S-valued points of X and G respectively, then $\pi(m(x_1g_1 \times x_2g_2)) = \pi(x_1g_1 \cdot x_2g_2) = \pi(x_1x_2g_3) = \pi(x_1x_2) = \pi(m(x_1 \times x_2))$ where $g_3 = (x_2^{-1}g_1x_2)\cdot g_2 \in \underline{G}(S)$. It is easy to check that the dotted

† *Normal* means $\underline{G}(S)$ is a normal subgroup of $\underline{X}(S)$ for every S.

arrow defines a group law m' on X/G in terms of which π is a homomorphism. Now since $G \times X \simeq X \times_Y X$, it follows that if $x_1, x_2 \in \underline{X}(S)$, then $\pi(x_1) = \pi(x_2)$ if and only if $x_1 = x_2 \cdot g$, some $g \in G(S)$. In particular, if $K = \text{kernel}(\pi)$,

$$x_1 \in \underline{K}(S) \iff \pi(x_1) = \pi(e) \iff x_1 = g, \text{ some } g \in \underline{G}(S).$$

Thus $G = \text{kernel}(\pi)$.

The second half of the corollary is harder. Let $\pi: X \to X/G$ be the canonical map. In view of the G-invariance of f, there is a unique $g: X/G \to Y$ such that

$$\begin{array}{ccc} & X & \\ {\scriptstyle\pi}\swarrow & & \searrow{\scriptstyle f} \\ X/G & \xrightarrow[g]{} & Y \end{array}$$

commutes. By the first half of the corollary, X/G is a group scheme, and one checks easily that g is a homomorphism. In fact, g is also an epimorphism with trivial kernel and we are reduced to proving the special case that an epimorphism $f: X \to Y$ with trivial kernel is an isomorphism. We recall that if $g: S \to T$ is any morphism such that $g^{-1}(t)$ is a finite set for every $t \in T$, then there is an open dense set $T_0 \subset T$ such that if $S_0 = g^{-1}(T_0)$ $g|_{S_0}: S_0 \to T_0$ is a finite morphism. In our case, say $f|_{X_0}: X_0 \to Y_0$ is finite. Then for every $x \in X$, if R_x is right translation by X, we get a diagram:

$$\begin{array}{ccc} X_0 & \xrightarrow{R_x} & X_0\cdot x \\ & \approx & \\ {\scriptstyle \text{res } f}\downarrow & & \downarrow{\scriptstyle \text{res } f} \\ & \approx & \\ Y_0 & \xrightarrow{R_{f(x)}} & Y_0\cdot f(x) \end{array}$$

so f is a finite morphism from $X_0 \cdot x$ to $Y_0 \cdot f(x)$ too. Since the open sets $Y_0 \cdot f(x)$ cover Y, f itself is a finite morphism. Therefore, to show that f is an isomorphism, it suffices to prove that the homo-

morphism $f^*: \mathcal{O}_Y \to f_*\mathcal{O}_X$ is an isomorphism. But we know f^* is injective, and by Nakayama's lemma, f^* is surjective if for all $y \in Y$, the map

$$f_y^*: k \approx \mathcal{O}_y/\mathfrak{M}_y \longrightarrow f_*\mathcal{O}_X \otimes_{\mathcal{O}_y} (\mathcal{O}_y/\mathfrak{M}_y)$$

is surjective. But $\mathrm{Spec}(f_*\mathcal{O}_X \otimes \mathcal{O}_y/\mathfrak{M}_y)$ is the fibre $f^{-1}(y)$, and all the fibres of f are isomorphic by translation to the kernel of f. This kernel is trivial, so we deduce that for all $y \in Y$, $f^{-1}(y)$ is one point with reduced structure. Therefore f_y^* is surjective, and f is an isomorphism.

COROLLARY 2. *Let $Y = X/G$ as in the theorem. Let $\mathfrak{g}$ be any coherent sheaf on X acted on by G. Then there is a natural isomorphism*

$$\pi^*(\pi_*\mathfrak{g}) \simeq \mathfrak{g} \otimes_k R.$$

PROOF. Given the situation:

$$\begin{array}{ccc} X' & \xrightarrow{g'} & X \\ {\scriptstyle f'}\downarrow & & \downarrow{\scriptstyle f} \\ Y' & \xrightarrow[g]{} & Y \end{array}$$

and a sheaf $\mathfrak{g}$ on X, the natural homomorphism $f^*(f_*(\mathfrak{g})) \to \mathfrak{g}$ induces $g'^*f^*(f_*(\mathfrak{g})) \to g'^*(\mathfrak{g})$, that is, $f'^*g^*(f_*(\mathfrak{g})) \to g'^*(\mathfrak{g})$, or what is the same, $g^*(f_*(\mathfrak{g})) \to f'_*(g'^*(\mathfrak{g}))$. If f is an affine morphism and $X' = Y' \times_Y X$, this is an isomorphism. In fact, the problem being local on Y and Y', we may assume both (and hence all four of X, Y, X', Y') affine, and the assertion is then obvious. Apply this remark with $X = Y'$, $f = g = \pi$, to deduce that $\pi^*(\pi_*(\mathfrak{g})) = p_{2*}p_1^*(\mathfrak{g})$ where $p_i: X \times_Y X \to X$ are the projections. Denoting the i^{th} projection of $G \times X$ by q_i, and using the isomorphism (μ, q_2): $G \times X \to X \times_Y X$ and the G-action on $\mathfrak{g}$, we get that $\pi^*(\pi_*(\mathfrak{g})) \simeq q_{2*}\mu^*(\mathfrak{g}) \simeq q_{2*}q_2^*(\mathfrak{g}) = \mathfrak{g} \otimes_k R$, which proves the corollary.

We now want to prove a theorem on the Euler characteristic of inverse images of coherent sheaves for a class of morphisms. For this, we introduce some definitions.

Let G be a finite group scheme acting freely on a scheme X such that the quotient X/G exists. Let F be a finite scheme on which G acts. Then G acts on $X \times F$ in an obvious way. It is easy to check that this action is again free, that the quotient $U = (X \times F)/G$ exists, and that we have a natural morphism $U \xrightarrow{\pi} V = X/G$. The morphism π obtained in this way will be called the *fibration with fiber F associated to the principal G-bundle $X \to X/G$*. π is finite and flat, so that $\pi_*(\mathcal{O}_U)$ is locally free over $\mathcal{O}_V$ of constant rank. We shall call this rank the *degree* of π.

THEOREM 2. *Let $\pi: U \to V$ be a fibration with finite fibers associated to a principal G-bundle over V, where G is a finite group scheme. For any coherent sheaf $\mathcal{F}$ on V, we have*

$$\chi(\pi^*(\mathcal{F})) = (\deg \pi) \cdot \chi(\mathcal{F}).$$

PROOF. It suffices to prove the theorem when G acts freely on U and $V = U/G$ since in the general case, we have $X \times F \to X \times F/G \to X/G$ and the theorem would be true for the composite and for the first morphism, so that it is also true for the second.

Thus we assume $V = U/G$ for a free action of G on U. For a coherent sheaf $\mathcal{F}$ on V, let $\mathcal{I}$ be the sheaf of ideals annihilating $\mathcal{F}$, and call the closed subschemes of V defined by $\mathcal{I}$ the support of $\mathcal{F}$. Then $\mathcal{F}$ is a coherent sheaf on this subscheme. If the theorem is not true, since V is a noetherian space, we can find an $\mathcal{F}$ with support $V' \subset V$ for which the theorem is not valid, whereas for any coherent $\mathfrak{g}$ with $\mathrm{Supp}\ \mathfrak{g} \subsetneq \mathrm{Supp}\ \mathcal{F}$, the theorem is valid. Set $U' = \pi^{-1}(V')$. Then, using (B) of the proposition, one sees that U' is a principal G-space over V'. Replacing U and V by U' and V' respectively, we see that we may assume the theorem to be valid whenever $\mathrm{Supp}\ \mathcal{F} \subsetneq V$, that is, whenever $\mathrm{Ann}\ \mathcal{F} \neq (0)$. It is further clear that if in a short exact sequence of coherent sheaves on V, the theorem holds for two of the sheaves, it holds for the third (remember π is flat).

Now, if V were reducible, we can find a short exact sequence $0 \to \mathcal{G}_1 \to \mathcal{F} \to \mathcal{G}_2 \to 0$ with $\mathcal{G}_i$ having proper support $\subsetneq V$, and the theorem would hold for $\mathcal{F}$. Hence we may suppose V irreducible. If $\mathcal{I}$ is the subsheaf of nilpotent elements of V and $\mathcal{I} \neq 0$ we have the exact sequence $0 \to \mathcal{I}.\mathcal{F} \to \mathcal{F} \to \mathcal{F}/\mathcal{I}.\mathcal{F} \to 0$ and both $\mathcal{I}.\mathcal{F}$ and $\mathcal{F}/\mathcal{I}.\mathcal{F}$ have supports proper closed subschemes of V. Thus we may assume V reduced and irreducible. Let r be the rank of the generic fiber of $\mathcal{F}$. Then there is a sheaf of ideals $\mathcal{I}$ on V and an injective homomorphism $\mathcal{I}^r \to \mathcal{F}$ with cokernel having proper support. Thus, the theorem holds for $\mathcal{F}$ if and only if it holds for $\mathcal{I}^r$, and again by the exact sequence $0 \to \mathcal{I} \to \mathcal{O}_V \to \mathcal{O}_V/\mathcal{I} \to 0$, we see that the theorem holds for $\mathcal{I}$ if and only if it holds for $\mathcal{O}_V$. We see therefore that it suffices to prove the theorem for *one* coherent sheaf on V of non-zero rank. But then, $\pi_*(\mathcal{O}_U)$ is such a sheaf, since by Corollary 2 to the proposition,

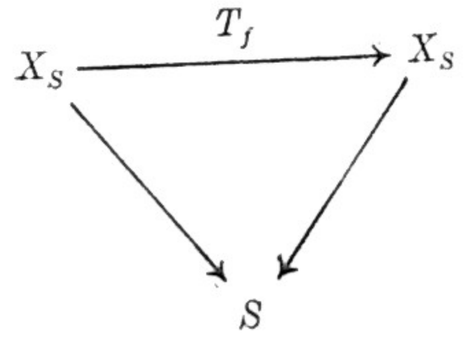
$$\chi(\pi^*(\pi_*(\mathcal{O}_U))) = \chi(\mathcal{O}_U \otimes_k R) = (\deg \pi)\, \chi(\mathcal{O}_U)$$
$$= (\deg \pi)\, \chi(\pi_*(\mathcal{O}_U)).$$

REMARK. The reason we have insisted on an associated fiber space, rather than confine ourselves to a space on which G acts freely is the following. Let $f\colon U \to V$ be a finite étale morphism everywhere of degree n. Then f can always be realized as the associated fiber space with finite fibers of a principal $\Sigma(n)$-space, where $\Sigma(n)$ is the symmetric group of order n. In fact, in the n-fold fiber product $U \times_V U \times_V \dots \times_V U$, consider the set P of points $(x_1, \dots, x_n)$ such that $x_i \neq x_j$ for $i \neq j$. Then P is both open and closed in $U \times_V U \times_V \dots \times_V U$ and is stable for the natural action of $\Sigma(n)$. Further, P is étale over V, and V is the set-theoretic quotient of P by $\Sigma(n)$. It clearly follows that V is the scheme-theoretic quotient of P by $\Sigma(n)$ and P is a principal fiber space with structure group $\Sigma(n)$ over V. Let F be the reduced scheme with n points $[1, 2, \dots, n]$ on which $\Sigma(n)$ acts naturally. Define a map $P \times F \to V$ by $((x_1, \dots, x_n), i) \longmapsto x_i$. This map is invariant for the action of $\Sigma(n)$ on $P \times F$ and V is the set-theoretic quotient. Since $P \times F \to V$ is again étale, V is the scheme quotient of $P \times F$ by $\Sigma(n)$.

Thus, the theorem is applicable to any finite étale morphism of constant degree n.

13. The Dual Abelian Variety in any characteristic. For a line bundle L on an abelian variety X, we had earlier defined a closed subset $K(L)$ of X as consisting of the points $x \in X$ for which $T_x^*(L) \simeq L$, and we had shown that it is a subgroup. We shall now define a structure of subscheme on $K(L)$. Namely, consider the standard line bundle $M = m^*(L) \otimes p_1^*(L)^{-1} \otimes p_2^*(L)^{-1}$ on $X \times X$, and define $K(L)$ to be the maximal subscheme of X such that $M | K(L) \times X$ is trivial. (See § 10).

We can interpret the S-valued points of $K(L)$ roughly as the set of S-valued points $f\colon S \to X$ such that L is invariant under translation by f. Namely, $X_S = X \times S$, and let T_f:



be the automorphism of X_S induced by f (i.e. $T_f(x, s) = (x + f(s), s)$ in terms of T-valued points x, s of X, S). Let L_S be the induced line bundle $p_1^* L$ on X_S. Now when S is a big space, the condition $T_f^*(L_S) \simeq L_S$ is too strong; for example, L_S and $T_f^*(L_S)$ can be isomorphic on the sets $X \times U_i$ for $\{U_i\}$ an open cover of S, without being isomorphic. The correct condition to look at is:

$$T_f^*(L_S) \simeq L_S \otimes p_2^* N, \qquad N \text{ a line bundle on } S. \qquad (*)$$

Then I claim that (*) holds if and only if f is an S-valued point of $K(L)$.

PROOF. Note that the composite $X \times S \xrightarrow{T_f} X \times S \xrightarrow{p_1} X$ is just the composite $X \times S \xrightarrow{1_X \times f} X \times X \xrightarrow{m} X$, so $T_f^*(L_S) \simeq (1_X \times f)^* m^* L$. Thus $L_S|_{(0) \times S}$ is trivial, while $T_f^*(L_S)|_{(0) \times S} \simeq f^* L$.

Now whenever (*) holds, the N which occurs can be identified by restricting both sides to $(0) \times S$:

$$f^*(L) \simeq T_f^*(L_S)\,|_{(0)\times S} \simeq L_S \otimes p_2^* N\,|_{(0)\times S} \simeq N.$$

Thus (*) holds if and only if

$$(1_X \times f)^* m^* L \simeq p_1^* L \otimes p_2^*(f^* L).$$

But $(1_X \times f)^* m^* L \otimes p_1^* L^{-1} \otimes p_2^*(f^*L)^{-1} \simeq (1_X \times f)^* M$, so (*) holds if and only if $(1_X \times f)^* M$ is trivial, which means, by definition that f factors through $K(L)$.

An immediate consequence is that $\underline{K(L)}\,(S)$ is a *subgroup* of $\underline{X}(S)$, hence $K(L)$ is a subgroup scheme of X.

Our next aim is to construct the dual abelian variety of X, imitating the procedure in characteristic 0. Choose an L which is ample. Then $K(L)$ is a finite group scheme. We define $\hat{X}$ to be the quotient abelian variety $X/K(L)$. Let $\pi: X \to \hat{X}$ be the natural homomorphism. As before, we wish to define the Poincaré line bundle P on $\hat{X} \times X$ by defining it as the quotient of the line bundle M on $X \times X$ by a suitable action of $K(L) \times \{0\}$ lifting the translation action on $X \times X$ (it is easily checked that the natural homomorphism $X \times X/K(L) \times \{0\} \xrightarrow{\sim} X/K(L) \times X$ is an isomorphism).

Recall that an action of a subgroup $H \subset X$ on any coherent sheaf $\mathscr{F}$ on X can be described as the giving, for each $S \in \mathrm{Obj}\ \underline{\mathrm{Sch}}$, an action of the (abstract) group $\underline{H}(S)$ on $\mathscr{F}_S = \mathscr{F} \otimes_k \mathcal{O}_S$ lifting the action on X_S, this action varying functorially in S in an obvious sense.

Let us agree to denote all objects obtained by base extension to S by a subscript S. Now, $\underline{K(L)}(S)$ consists of the subgroup of $x \in \underline{X}(S)$ such that if T_x: $X_S \to X_S$ denotes translation by x, $T_x^*(L_S) \simeq L_S \otimes L_0$, where L_0 is the lift to X_S of a line bundle on S. On $X_S \times_S X_S = (X \times X)_S$, $M_S \simeq m_S^*(L_S) \otimes p_1^*(L_S)^{-1} \otimes p_2^*(L_S)^{-1}$, so that $T_{(x,0)}^*(M_S) \simeq m_S^* T_x^*(L_S) \otimes p_1^* T_x^*(L_S)^{-1} \otimes p_2^*(L_S)^{-1} \simeq M_S \otimes m_S^*(L_0) \otimes p_1^*(L_0^{-1}) \simeq M_S$. Thus, $T_{(x,0)}^*(M_S) \simeq M_S$, and to define a lift of $T_{(x,0)}$ to M_S, or equivalently an isomorphism of $T_{(x,0)}^*(M_S)$ with M_S,

it suffices to give an isomorphism of these line bundles on the subscheme $X_S \times_S 0_S$. This is because any two isomorphisms, either on $X_S \times_S X_S$ or on $X_S \times_S 0_S$, differ by multiplication by a unit, and the groups of global units on these schemes, $H^0((X \times X)_S, \mathcal{O}^*_{(X\times X)_S})$ and $H^0(X_S \times_S 0_S,\ \mathcal{O}^*_{X_S \times_S 0_S})$, are both isomorphic to $H^0(S, \mathcal{O}_S^*)$, hence the restriction map $H^0((X \times X)_S, \mathcal{O}^*_{(X\times X)_S}) \xrightarrow{\sim} H^0(X_S \times_S 0_S, \mathcal{O}^*_{X_S \times_S 0_S})$ is an isomorphism. Next, let V be the 1-dimensional vector space dual to the fiber $L/\mathfrak{M}_0 L$ of L at 0 on X, and let $V \times X_S$ be the trivial line bundle over X_S with fibre V. Then, if i: $X_S = X_S \times_S 0_S \to X_S \times_S X_S$ is the closed immersion,

$$i^*(M_S) \simeq i^* m^*(L_S) \otimes i^* p_1^*(L_S)^{-1} \otimes i^* p_2^*(L_S)^{-1} \simeq L_S \otimes L_S^{-1} \otimes_k V \simeq V \times X_S,$$

where all the isomorphisms are *canonical*. Therefore, we can choose a unique lifting of the translation $T_{(X,0)}$ to M_S by requiring that this lifting when restricted to $X_S \times_S 0_S$, becomes the map $1_V \times T_x$ on $V \times X_S$. It is then easy to check that the action of $\underline{K(L)}(S)$ on M_S defined like this is a group action, as required.

We conclude that there is a unique line bundle P on $\hat{X} \times X = X/K(L) \times X$ such that its pull back is isomorphic, as a line bundle acted on by $K(L)$, to M on $X \times X$. The restrictions of P to $\{0\} \times X$ and $\hat{X} \times \{0\}$ are trivial. Further, since ϕ_L: $X \to \mathrm{Pic}^0 X$ is surjective with kernel $K(L)$ we see that there is an induced isomorphism of abstract groups $\hat{X} \xrightarrow{\sim} \mathrm{Pic}^0 X$, and if $\alpha \in \hat{X}$, the restriction of P to $\{\alpha\} \times X$, considered as a line bundle on X, is nothing but the element of $\mathrm{Pic}^0 X$ corresponding to α. Thus, to check that $\hat{X}$ is a dual variety and P a Poincaré bundle on $\hat{X} \times X$, we have to prove the following

THEOREM. *Let S be any scheme, and L a line bundle on $S \times X$ such that $L\,|\,S \times \{0\}$ is trivial and $L\,|\,\{s\} \times X \in \mathrm{Pic}^0 X$ for every $s \in S$. Then there is a unique morphism ϕ: $S \to \hat{X}$ such that $L \simeq (\phi \times 1_X)^*(P)$.*

PROOF. Consider the line bundle $M = p_{23}^*(P) \otimes p_{13}^*(L)^{-1}$ on $S \times \hat{X} \times X$, and let Γ_S be the maximal subscheme of $S \times \hat{X}$

over which this line bundle is trivial. The main point is to show that if $\pi: \Gamma_S \to S$ is the restriction to Γ_S of the projection $S \times X \to S$, π is an isomorphism. For this, it is clearly sufficient to show that for any closed subscheme S_0 of S having support at one point of S, $(S_0 \times_S \Gamma_S) \to S_0$ is an isomorphism. On the other hand, by definition of Γ_S, if Γ_{S_0} denotes the corresponding closed subscheme of $S_0 \times X$ formed with respect to the line bundle $L \mid S_0 \times X$ on $S_0 \times X$, we have $S_0 \times_S \Gamma_S = \Gamma_{S_0}$. Thus for the proof of the main point, we may assume $S = \operatorname{Spec} B$, where B is a finite-dimensional local k-algebra. Further, if s is the unique point of S, one sees easily that the statement to be proved remains unaltered if we replace L by $L \otimes p_2^*(L \mid \{s\} \times X)^{-1}$, (since $\exists\ \hat{x} \in \hat{X}$ such that $L \mid \{s\} \times X \simeq P \mid \{\hat{x}\} \times X$) so that we may further assume that $L \mid \{s\} \times X$ is trivial.

Now, for all points $(s, x) \in S \times X$, the restriction of M to $\{s\} \times \hat{X} \times \{x\}$ belongs to $\operatorname{Pic}^0 \hat{X}$ (since this is so for $(s, 0)$); and there are at most finitely many points (s, x) such that M restricted to $\{s\} \times \hat{X} \times \{x\}$ is trivial, since there are at most finitely many $x \in X$ such that $m^*(L) \otimes p_1^*(L)^{-1} \otimes p_2^*(L)^{-1} \mid X \times \{x\} = T_x^*(L) \otimes L^{-1}$ is trivial. Hence, all the direct images $R^p p_{13,*}(M)$ on $S \times X$ have discrete support, so that by the Leray spectral sequence, $H^p(S \times \hat{X} \times X,\ M) \simeq H^0(S \times X, R^p p_{13,*}(M))$. On the other hand, $R^p p_{13,*}(M) \simeq R^p p_{13,*}(p_{23}^*(P)) \otimes L^{-1}$, so that we have isomorphisms of B-modules $H^p(S \times \hat{X} \times X, M) \simeq H^p(S \times \hat{X} \times X,\ p_{23}^*(P)) \simeq B \otimes_k H^p(\hat{X} \times X,\ P), p \geqslant 0$.

Therefore these cohomology groups are free B-modules. On the other hand, consider the direct images $R^p p_{12,*}(M)$. Since $M \mid \{s\} \times \{\hat{x}\} \times X \in \operatorname{Pic}^0 X$ for all $\hat{x}$ and is trivial only for $\hat{x} = 0$, all these sheaves $R^p p_{12,*}(M)$ are concentrated at the point $(s, 0) \in S \times \hat{X}$. Let $0 \to K_0 \to K_1 \to \dots \to K_g \to 0$ be a complex of free modules of finite type over the local ring $A = B \otimes_k \mathcal{O}_{0,\hat{X}}$ of $(s,0) \in S \times \hat{X}$ given by the base change theorem for direct images. Then $H^i(K.) \simeq [R^i p_{12,*}(M)]_{(s,0)}$ are modules of finite length over A and hence also over $\mathcal{O}_{0,\hat{X}}$. Now we have the

LEMMA. *Let $\mathcal{O}$ be a regular local ring of dimension g, and $0 \to K_0 \to K_1 \to \dots \to K_g \to 0$ be a complex of finitely generated free modules over $\mathcal{O}$. If the $H^i(K.)$ are artinian modules, we have $H^i(K.) = 0$ for $0 \leqslant i < g$.*

PROOF. Since there is nothing to prove for $g = 0$, we may assume $g > 0$ and that the result holds in smaller dimensions. Choose an x in the maximal ideal $\mathfrak{M}$ of $\mathcal{O}$ but not in $\mathfrak{M}^2$, so that $\overline{\mathcal{O}} = \mathcal{O}/\mathcal{O}x$ is regular of dimension $g - 1$. Putting $\overline{K}. = \overline{\mathcal{O}} \otimes_{\mathcal{O}} K.$, we have the exact sequence of complexes $0 \longrightarrow K. \xrightarrow{x} K. \longrightarrow \overline{K}. \longrightarrow 0$, from which we get the exact sequence

$$H^p(K.) \xrightarrow{x} H^p(K.) \longrightarrow H^p(\overline{K}.) \longrightarrow H^{p+1}(K.) \xrightarrow{x} H^{p+1}(K.).$$

This shows that the $H^p(\overline{K}.)$ are artinian. By induction hypothesis, $H^p(\overline{K}.) = 0$ for $p < g - 1$, so $H^{p+1}(K.) \xrightarrow{x} H^{p+1}(K.)$ is injective for $p < g - 1$. But since $H^{p+1}(K.)$ is artinian, x^n kills $H^{p+1}(K.)$ for some n, and hence $H^{p+1}(K.) = 0$, $p < g - 1$. The lemma is proved.

Applying the lemma to our complex of A free (and hence $\mathcal{O}_{0,\hat{X}}$-free) modules above, we deduce that $R^i p_{12,*}(M) = 0$ for $0 \leqslant i < g$, and that $0 \to K_0 \to K_1 \to \dots \to K_g \to N \to 0$ is an exact sequence of A-modules, where $N = R^g p_{12,*}(M)_{(s,0)} \simeq H^g(S \times \hat{X} \times X,\ M)$, which we saw above is B-free. Now, the derived modules of the complex $0 \to \hat{K}_g \to \hat{K}_{g-1} \to \dots \to \hat{K}_0 \to 0$, where $\hat{K}_i = \operatorname{Hom}_A(K_i, A)$, are again artinian, so that by another application of the above lemma, we get an exact sequence $0 \to \hat{K}_g \to \dots \to \hat{K}_0 \to K \to 0$, where K is an artinian A-module. Since we have the exact sequence

$$\begin{array}{ccccccc} & & & & k & & \\ & & & & \wr\| & & \\ 0 & \longrightarrow & H^0(\{s\} \times \{0\} \times X,\ P\,|_{\{s\} \times \{0\} \times X}) & \longrightarrow & K_0 \otimes_A k & \longrightarrow & K_1 \otimes_A k \end{array}$$

we get that the cokernel of $\hat{K}_1 \otimes k \to \hat{K}_0 \otimes k$ is of dimension one over k, that is, $K \otimes_A k = K/\mathfrak{M}_A K$ is one-dimensional. Therefore,

$K \simeq A/\mathfrak{A}$ as an A-module, for an ideal $\mathfrak{A}$ of A, and the free complex $(\hat{K}_i)$ resolves $A/\mathfrak{A}$. This implies that the homologies of its dual complex (K_i) are also annihilated by $\mathfrak{A}$, that is, $\mathfrak{A}.N = 0$†. Since N is B-free, $\mathfrak{A} \cap B \otimes 1 = (0)$, that is, $B \to A/\mathfrak{A}$ is injective. For any $\mathfrak{M}$-primary ideal $\mathfrak{b}$ in A, if $V(\mathfrak{b})$ is the closed subscheme defined by $\mathfrak{b}$ in $S \times \hat{X}$, we have

$$H^0(V(\mathfrak{b}) \times X, M|_{V(\mathfrak{b})\times X}) \simeq \mathrm{Ker}[K_0/\mathfrak{b}K_0 \to K_1/\mathfrak{b}K_1] \simeq \mathrm{Hom}_A(A/\mathfrak{A}, A/\mathfrak{b}),$$

from which it follows that $V(\mathfrak{A})$ contains the maximal subscheme Γ_S of $S \times \hat{X}$ over which M is trivial. On the other hand, $H^0(V(\mathfrak{A}) \times X, M|_{V(\mathfrak{A})\times X} \simeq \mathrm{Hom}_A(A/\mathfrak{A}, A/\mathfrak{A}) \simeq A/\mathfrak{A}$, and the natural map of line bundles

$$\mathcal{O}_{V(\mathfrak{A})\times X} \otimes_{A/\mathfrak{A}} H^0(V(\mathfrak{A}) \times X, M|_{V(\mathfrak{A})\times X}) \to M|_{V(\mathfrak{A})\times X}$$

is surjective, since reduced modulo the maximal ideal, the induced map on sections

$$\begin{array}{ccc} \mathrm{Hom}_A(A/\mathfrak{A}, A/\mathfrak{A}) & & \mathrm{Hom}_A(A/\mathfrak{A}, A/\mathfrak{M}_A) \\ \wr\| & & \wr\| \\ H^0(V(\mathfrak{A}) \times X, M|_{V(\mathfrak{A})\times X}) & \longrightarrow & H^0(\{s\} \times \{0\} \times X, M|_{\{s\}\times\{0\}\times X}) \end{array}$$

is surjective, and the line bundle $M|_{\{s\}\times\{0\}\times X}$ is trivial. Hence, $M|_{V(\mathfrak{A})\times X}$ is trivial, which shows that $\Gamma_S = V(\mathfrak{A})$. In particular, $B \to H^0(\Gamma_S, \mathcal{O}_{\Gamma_S}) = A/\mathfrak{A}$ is injective. On the other hand, $\pi^{-1}(s)$ is a closed subscheme of $\Gamma_S \cap \{s\} \times X$ such that the restriction of $\{s\} \times P$ to $\pi^{-1}(s) \times X$ is trivial. Since $\{0\}$ is the maximal subscheme of $\hat{X}$ over which P is trivial (practically by construction of $\hat{X}$), $\pi^{-1}(s)$ becomes the reduced point $(s, 0)$. This means that $A/\mathfrak{A} + \mathfrak{M}_B A = k$, so that $B \to A/\mathfrak{A}$ is also surjective, hence an isomorphism. Thus, π: $\Gamma_S \to S$ is an isomorphism.

Now, for any scheme S and line bundle L on $S \times X$ satisfying the hypothesis of the theorem, and any morphism ϕ: $S \to \hat{X}$, denoting by Γ_ϕ: $S \to S \times \hat{X}$ the graph morphism, we have the

† In fact, for every $a \in \mathfrak{A}$, show that the endomorphism of $(\hat{K}_1)$ given by multiplication by a is null-homotopic; hence so is the same endomorphism of (K_i).

equivalence $(\phi \times 1_X)^*(P) \simeq L \iff \Gamma_\phi$ factors through Γ_S. So the theorem clearly follows from the fact that Γ_S is already the graph of a unique morphism from S to $\hat{X}$.

COROLLARY 1. *We have*

$$H^i(\hat{X} \times X, P) = \begin{cases} (0) & \text{if } i \neq g \\ k & \text{if } i = g. \end{cases}$$

PROOF. Using the notations of the proof of the theorem, with $B = k$, L trivial, we have established that $K \simeq k$, i.e.

$$0 \longrightarrow \hat{K}_g \longrightarrow \hat{K}_{g-1} \longrightarrow \cdots \longrightarrow \hat{K}_0 \longrightarrow k \longrightarrow 0$$

is a free resolution of k. On the other hand, any two free resolutions of one module are homotopically equivalent, and the residue field k of any regular local ring such as $\mathcal{O}_{0,\hat{X}}$ has a well-known standard resolution, the Koszul complex. Namely, let $x_1, \ldots, x_g \in \mathfrak{M}_0$ lift a basis $\{\overline{x}_i\}$ of $\mathfrak{M}_0/\mathfrak{M}_0^2$. Let L_k be the free $\mathcal{O}_{0,\hat{X}}$-module with the formal symbols $e_{i_1} \wedge \cdots \wedge e_{i_k}$ $(1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant g)$ as a basis. Then

$$0 \longrightarrow L_g \xrightarrow{d_g} L_{g-1} \xrightarrow{d_{g-1}} \cdots\cdots\cdots \xrightarrow{d_1} L_0 \xrightarrow{d_0} k \longrightarrow 0$$

$$d_k(e_{i_1} \wedge \cdots \wedge e_{i_k}) = \sum_{l=1}^{k} (-1)^l x_{i_l} e_{i_1} \wedge \cdots \wedge \hat{e}_{i_l} \wedge \cdots \wedge e_{i_k}$$

is the Koszul complex. Then the dual complex

$$0 \longrightarrow K_0 \longrightarrow K_1 \longrightarrow \cdots\cdots \longrightarrow K_g \longrightarrow 0$$

is homotopic to the dual of the Koszul complex, which it is easy to see is still isomorphic to the original Koszul complex. This gives Corollary 1 by calculating cohomologies.

COROLLARY 2. *For an abelian variety X of dimension g,*

$$\dim_k H^p(X, \mathcal{O}) = \binom{g}{p}.$$

PROOF. In fact, $H^p(X, \mathcal{O})$ is isomorphic to the p^{th} cohomology of the complex

$$\mathcal{O} \longrightarrow K_0 \otimes k \longrightarrow K_1 \otimes k \longrightarrow \cdots \longrightarrow K_g \otimes k \longrightarrow 0,$$

which is homotopic to the Koszul complex tensored with k. Now, the differential operators of the Koszul complex tensored with k are trivial, so that we have $\dim_k H^p(X, \mathcal{O}) =$ rank of module of p-cochains of Koszul complex $= \binom{g}{p}$.

COROLLARY 3. *There is a canonical isomorphism of the tangent space to* (0) *on* $\hat{X}$ *and* $H^1(X, \mathcal{O}_X)$.

PROOF. Let $S = \operatorname{Spec} \frac{k[\epsilon]}{(\epsilon^2)}$, so that the tangent space to $\hat{X}$ at 0 is canonically isomorphic to $\operatorname{Hom}_0(S, \hat{X})$, where Hom_0 denotes the set of morphisms of S into $\hat{X}$ mapping the unique point s_0 of S onto 0. On the other hand, we have by the theorem,

$$\begin{aligned}\operatorname{Hom}_0(S, \hat{X}) &= \{\text{Line bundles on } S \times X \text{ trivial on } \{s_0\} \times X\} \\ &= \ker\{H^1(S \times X, \mathcal{O}^*_{S\times X}) \longrightarrow H^1(\{s_0\} \times X, \mathcal{O}^*_X)\}.\end{aligned}$$

But now, we have an exact sequence of multiplicative sheaves

$$1 \longrightarrow 1 + \epsilon\, \mathcal{O}_X \longrightarrow \mathcal{O}^*_{S\times X} \longrightarrow \mathcal{O}^*_X \longrightarrow 1\,,$$

and as sheaves of abelian groups, $1 + \epsilon\, \mathcal{O}_X \simeq \mathcal{O}_X$. Therefore the cohomology sequence gives

$$0 \longrightarrow H^1(\mathcal{O}_X) \longrightarrow H^1(S \times X, \mathcal{O}^*_{S\times X}) \longrightarrow H^1(X, \mathcal{O}^*_X)$$

and this gives a natural isomorphism of the tangent space to 0 at $\hat{X}$ with $H^1(X, \mathcal{O}_X)$, at least as abelian groups. It can be checked that this is actually an isomorphism of k-vector spaces.

Now, let $f\colon X \to Y$ be an isogeny of abelian varieties. By the theorem, we get a unique homomorphism $\hat{f}\colon \hat{Y} \to \hat{X}$ of abelian varieties such that if P_X, P_Y are the Poincaré bundles on $X \times \hat{X}$ and $Y \times \hat{Y}$ respectively, we have

$$(1 \times \hat{f})^*(P_X) \simeq (f \times 1)^*(P_Y).$$

Hence, if we denote this line bundle by Q, on applying the proposition of §12, we get that

$$\chi(Q) = \deg \hat{f} \cdot \chi(P_X) = \deg f \cdot \chi(P_Y),$$

and since $\chi(P_X) = \chi(P_Y) = (-1)^g$ by Corollary 1, we get

COROLLARY 4. *For an isogeny* $f\colon X \to Y$ *of abelian varieties,*

$$\deg f = \deg \hat{f}.$$

COROLLARY 5. *For every line bundle* L *on* X, *the set-theoretic homomorphism* $\phi_L\colon X \to \operatorname{Pic}^0 X \approx \hat{X}$ *is a morphism, and* $K(L)$, *with its scheme structure as above, is its kernel.*

PROOF. In fact, ϕ_L is the unique morphism from X to $\hat{X}$ such that

$$(\phi_L \times 1_X)^* P \simeq m^* L \otimes p_1^* L^{-1} \otimes p_2^* L^{-1}.$$

Now by definition $K(L)$ is the largest subscheme S of X such that the bundle on the right is trivial on $S \times X$; and in view of the Universal Mapping Property of X, $\ker(\phi_L)$ is the largest subscheme S of X such that the bundle on the left is trivial on $S \times X$.

SYMMETRIC DEFINITION OF $\hat{X}$.

We wish to set up the relations between X and $\hat{X}$ in an obviously symmetric way. Define a *divisorial correspondence* between two abelian varieties X, Y of the same dimension to be a line bundle on $X \times Y$ whose restrictions to $\{0\} \times Y$ and $X \times \{0\}$ are trivial.

PROPOSITION. *For a divisorial correspondence* Q *between* X *and* Y, *the following are equivalent.*

(a) *There is no subscheme* Z *of* X *different from* (0) *such that the restriction of* Q *to* $Z \times Y$ *is trivial.*

(b) *There is no subscheme* Z' *of* Y *different from* (0) *such that* Q *restricted to* $X \times Z'$ *is trivial.*

(c) *The absolute value of* $\chi(Q)$ *is* 1.

When these conditions hold, Y *is canonically isomorphic to the dual of* X, *and* X *is canonically isomorphic to the dual of* Y.

PROOF. By symmetry, it suffices to show that (b) $\Longleftrightarrow$ (c). Now, we get a morphism $f : Y \longrightarrow \hat{X}$ such that $(1_X \times f)^*(P) = Q$. Now, f

has to be a homomorphism since $f(0) = 0$. Clearly, (b) is equivalent to saying that f has trivial kernel. If this holds, then since $\dim Y = \dim X = \dim \hat{X}$, f is an isogeny, hence by Corollary 1, §12, f is an isomorphism. Thus we have to show that f is an isomorphism if and only if $|\chi(Q)| = 1$. By Theorem 2 of §12, if f is an isogeny,

$$|\chi(Q)| = (\deg f).|\chi(P)| = \deg f$$

and the result follows. On the other hand, if f has positive dimensional kernel we can choose a finite subgroup $F \subset \ker(f)$ of arbitrarily large order d. The map $1_X \times f: X \times Y \longrightarrow X \times \hat{X}$ factors as

$$X \times Y \longrightarrow X \times Y/F \longrightarrow X \times \hat{X},$$

so that Q is the pull-back of a line bundle on $X \times Y/F$. Therefore $d \mid |\chi(Q)|$ by Theorem 2, §12, and since this holds for arbitrarily large d, $\chi(Q) = 0$.

COROLLARY. (The duality hypothesis.) *For any abelian variety X, the canonical morphism $i: X \to \hat{\hat{X}}$ defined by the Poincaré bundle P on $X \times \hat{X}$ (regarded as a family of line bundles on $\hat{X}$ parametrized by X) is an isomorphism.*

PROOF. In fact, the divisorial correspondence P on $X \times \hat{X}$ fulfils (b) (or (c)), hence also (a).

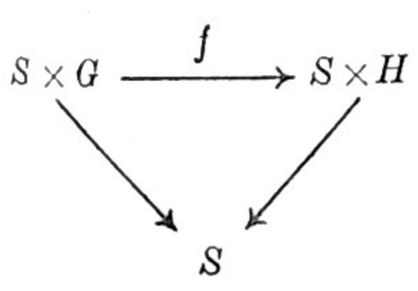
14. Duality Theory of Finite Commutative Group Schemes. Throughout this section, the ground field k is assumed algebraically closed, of positive characteristic $p > 0$.

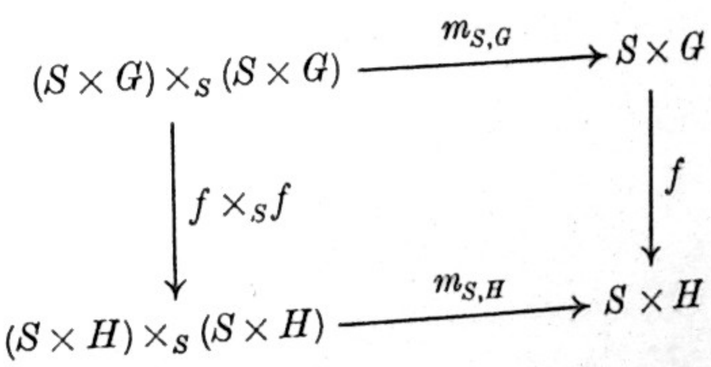
Let G be a finite commutative group scheme, so that G is affine, hence $G = \mathrm{Spec}\,(R)$, where R is a finite-dimensional k-algebra. The group law gives us a map $\mu: R \to R \otimes_k R$, the inverse gives us a map $i: R \to R$, and evaluation at the identity e gives us an augmentation $\delta: R \to k$. In the present case, the hyperalgebra $\mathbf{H}$ of G is simply the dual vector space R^* of R, and we will use the notation R^* instead of $\mathbf{H}$. As in §11, the group law μ dualizes to an associative multiplication

$$\mu^*: R^* \otimes_k R^* \longrightarrow R^*.$$

Since G is commutative, μ is co-commutative and so μ^* is commutative i.e. R^* is also a finite-dimensional commutative k-algebra. As in §11, the linear functional δ is the identity element of R^*. On the other hand, if $m: R \otimes_k R \to R$ is the multiplication of R, then $m^*: R^* \to R^* \otimes_k R^*$ will be a co-associative, co-commutative map. Together with the dual $i^*: R^* \to R^*$ of i, we get a group law and an inverse making the scheme $\hat{G} = \mathrm{Spec}\ R^*$ into a second finite commutative group scheme. The identity *point* of $\hat{G}$ corresponds to the homomorphism $R^* \to k$ gotten by evaluating linear functionals at $1 \in R$. Thus, to every finite commutative group scheme G we have associated in a canonical fashion another finite commutative group scheme $\hat{G}$, which we shall call the dual of G. This construction is due to Cartier. We shall now give a more 'geometric' definition (cf. Oort [O]).

For group schemes G and H and any scheme S, let $\mathrm{Hom}_S(G, H)$ denote the set of morphisms $f: S \times G \to S \times H$ such that the diagrams





are commutative, where $m_{S,G}$ and $m_{S,H}$ are the multiplications of G and H lifted to $S \times G$ and $S \times H$ respectively. Such morphisms f will be called S-homomorphisms from G to H. One checks easily that if H is commutative, $\mathrm{Hom}_S(G, H)$ can be made into a commutative group by defining $f + g = m_{S,H} \circ (f, g)$. Given a morphism $T \to S$, we have an associated homomorphism $\mathrm{Hom}_S(G, H) \to \mathrm{Hom}_T(G, H)$

given by $f \longmapsto f \times_S T$, so that for given G, H, we get a functor $\underline{\mathrm{Sch}} \to \underline{\mathrm{Sets}}$ given by $S \longmapsto \mathrm{Hom}_S(G, H)$, and this is in fact a commutative group-valued functor when H is commutative.

Now suppose $G = \mathrm{Spec}\ A$ is a finite commutative group scheme and H the multiplicative group scheme $\mathbf{G}_m$. We then assert that the functor $\underline{\mathrm{Sch}} \to \underline{\mathrm{Ab}}$, $S \longmapsto \mathrm{Hom}_S(G, \mathbf{G}_m)$ is represented by $\hat{G}$, that is, there is for each S an isomorphism

$$\underline{\hat{G}}(S) \simeq \mathrm{Hom}_S(G, \mathbf{G}_m),$$

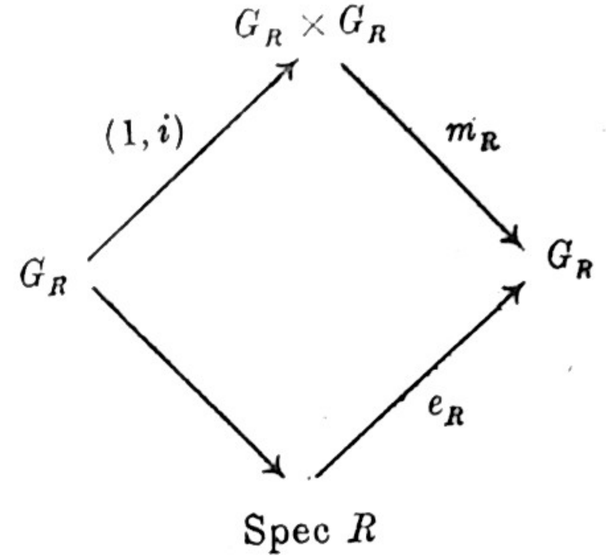
which is functorial in S. Now, if we restrict S to vary in the open subsets of a fixed scheme, it is clear that both sides define sheaves on this scheme. Hence by standard arguments, it suffices to establish the above isomorphism as S varies through affine schemes, $S = \mathrm{Spec}\ R$. Let us denote as usual the objects, morphisms, etc., obtained after base extension to R by a subscript R. Then the coordinate rings of G_R and $\mathbf{G}_{mR}$ become bi-algebras over R, that is, they are algebras with 1 over R, with co-multiplication maps $A_R \to A_R \otimes_R A_R$, etc., satisfying the usual identities, and co-identity maps $A_R \to R$, etc. The notion of homomorphism of bialgebras is then clear. We then have

$$\underline{\hat{G}}(R) = \mathrm{Hom}\,(\mathrm{Spec}\ R, \hat{G}) = \mathrm{Hom}_{k\text{-alg}}(A^*, R) = \mathrm{Hom}_{R\text{-alg}}(R \otimes_k A^*, R)$$
$$= \mathrm{Hom}_{R\text{-alg}}((A_R)^*, R),$$

where $(A_R)^*$ is the R-algebra $\mathrm{Hom}_R(A_R, R)$. Further,

$$\mathrm{Hom}_R(G, \mathbf{G}_m) = \mathrm{Hom}_{R\text{-bialg}}(R[T, T^{-1}], A_R) \xrightarrow{\ i\ } A_R,$$

where i is the inclusion defined by $i(\phi) = \phi(T)$. Clearly, an element $\alpha \in A_R$ is in the image of i if and only if (i) α is a unit in A_R, and (ii) $\mu_R(\alpha) = \alpha \otimes \alpha$. But in the presence of assumption (ii), (i) is equivalent to (i)′ $\epsilon_R(\alpha) = 1$, where $\epsilon_R : A_R \to R$ is the homomorphism given by the identity. In fact, (i) implies that $\epsilon_R(\alpha)$ is a unit, and on the other hand $(\epsilon_R \otimes \epsilon_R)(\mu_R(\alpha)) = \epsilon_R(\alpha)$, that is, $\epsilon_R(\alpha)^2 = \epsilon_R(\alpha)$, so that $\epsilon_R(\alpha) = 1$; on the other hand, if (i)′ and (ii) hold and $i^* : A_R \to A_R$ is got from the inverse, we have commutativity of the diagram



and taking the pull-back of the function α by these maps, we find $\alpha . i^*(\alpha) = 1$, so that α is a unit. Now, since A_R is R-free of finite rank we have a natural isomorphism

$$A_R \xrightarrow{\ \sim\ } \mathrm{Hom}_R((A_R)^*, R)$$

and under this isomorphism, elements α satisfying (i)′ and (ii) go over into element $f \in \mathrm{Hom}_R((A_R)^*, R)$ such that $f(1) = 1$ and $f(XY) = f(X).f(Y)$ for $X, Y \in (A_R)^*$ (since $XY = \mu_R^*(X \otimes Y)$). Thus we have set up a set-theoretic bijection between $\underline{\hat{G}}(R)$ and $\mathrm{Hom}_R(G, \mathbf{G}_m)$ natural in R. We leave it to the reader to check that this is an isomorphism of groups.

In particular, taking $S = \hat{G}$ in the above isomorphism, we get a morphism $\hat{G} \times G \to \mathbf{G}_m$ corresponding to the identity of $\underline{\hat{G}}(\hat{G})$, defined by the homomorphism of k-algebras $k[T, T^{-1}] \to A^* \otimes_k A$, $T \longmapsto \delta$, $\delta =$ the 'diagonal element' of $A^* \otimes_k A$ (which corresponds to $1_A \in \mathrm{Hom}_k(A, A)$ under the natural isomorphism $A^* \otimes_k A \xrightarrow{\ \sim\ } \mathrm{Hom}_k(A, A)$). One checks easily from this that this 'universal character' $\hat{G} \times G \to \mathbf{G}_m$ is in fact a bilinear map of group schemes in the obvious sense.

EXAMPLES. (1) Suppose G is a discrete (i.e. reduced) finite group of order n prime to p. By the above, the geometric points of $\hat{G}$ form a group isomorphic to $\mathrm{Hom}(G, k^*)$, which is of order n.

On the other hand, if A is the ring of functions of G, $\dim A = \dim A^* = n$, which shows that $\hat{G}$ is again reduced, and is isomorphic as a discrete group to $\mathrm{Hom}(G, k^*)$.

(2) Next suppose G is reduced and isomorphic to $\mathbf{Z}/p^n\mathbf{Z}$. For any reduced G let $k[G]$ be the group algebra of G. If we identify any $g \in G$ with the linear form $A \to k$ which is evaluation at g, we get an isomorphism of vector spaces $k[G] \xrightarrow{\sim} A^*$, which is trivially seen to be an isomorphism of algebras. Hence $\hat{G}$ has coordinate ring A^* isomorphic to the group algebra of $\mathbf{Z}/p^n\mathbf{Z}$, i.e. $A^* \simeq k(X)/(X^{p^n} - 1)$, where X corresponds to evaluation at the generator $\overline{1} \in \mathbf{Z}/p^n\mathbf{Z}$. On the other hand, for $f, g \in A$, $\overline{1}(f \cdot g) = (fg)(\overline{1}) = f(\overline{1}) \cdot g(\overline{1}) = (\overline{1} \otimes \overline{1})(f \otimes g)$, which shows that the co-multiplication on A^* is given by $X \longmapsto X \otimes X$. Thus we have an isomorphism.

$$\widehat{(\mathbf{Z}/p^n\mathbf{Z})} \simeq \mu_{p^n},$$

hence also

$$\widehat{(\mu_{p^n})} \simeq \mathbf{Z}/p^n\mathbf{Z}.$$

Now, let G be any finite commutative group scheme. We shall say that G is of type l(local) or r(reduced) if the underlying space of G is a single point or if G is reduced respectively. We shall say that G is of type (l, l) (resp. (l, r), (r, l), (r, r)) if G is of type l and $\hat{G}$ is of type l(resp. G of type l, $\hat{G}$ of type r; etc.). We shall show that any group admits a unique decomposition as a product

$$G = G_{r,r} \times G_{r,l} \times G_{l,r} \times G_{l,l}$$

of groups of the indicated types. In fact, if G^0 is the connected component of identity in G, considered as an open and closed subscheme, and if G_{red} is the reduced group, the closed immersions $G^0 \hookrightarrow G$ and $G_{\mathrm{red}} \hookrightarrow G$ induce a homomorphism $G^0 \times G_{\mathrm{red}} \to G$ which is clearly an isomorphism. Further, this decomposition of G into the product of a reduced and a local group is clearly unique. Thus, it suffices to show that each local (resp. reduced) group is uniquely expressible as a product $G_{lr} \times G_{ll}$ (resp. $G_{rr} \times G_{rl}$). Now, if G is reduced, G is uniquely expressible as a product $G_1 \times G_2$ where G_1 is of order prime to p and G_2 is a p-group. By the above, $\hat{G}_1$ is again reduced and $\hat{G}_2$ is local, which proves the assertion for reduced groups. When G is local, split $\hat{G}$ into its local and reduced parts. Dualizing back, this implies a unique decomposition of a local G into groups of type (l, r) and (l, l) respectively. This proves the assertion for local groups.

It follows from our discussion that the only groups of type (r, r) are those reduced groups of orders prime to p, hence direct products of cyclic prime power groups, the primes being distinct from p; that the only groups of type (r, l) are p-groups, hence direct products of $\mathbf{Z}/p^{n_i}\mathbf{Z}$'s; and that the only groups of type (l, r) are duals of p-groups, hence direct products of $\mu_{p^{n_i}}$'s.

There are plenty of examples of local-local groups. For instance, the groups α_{p^n} are local-local. In fact, since Spec $\dfrac{k[X]}{(X^{p^n})}$ cannot be decomposed as a product (the tangent space being one-dimensional), it suffices to see that it is not isomorphic to μ_{p^n}. Since α_p is a quotient of α_{p^n}, it even suffices to see that α_p is not isomorphic to μ_p. But now, if ξ is the linear form on $A = k[X]/(X^p)$ defined by

$$\xi(x^i) = \begin{cases} 0 \text{ if } i \neq p-1 \\ 1 \text{ if } i = p-1 \end{cases} \quad \text{in } A^*,$$

we have $\xi^2(X^i) = (\xi \otimes \xi)((1 \otimes X + X \otimes 1)^i) = 0$ if $i < p - 1$, which shows that A^* has nilpotent elements.

So far we have developed the circle of ideas involving homomorphisms from G to $\mathbf{G}_m$. Next we turn to homomorphisms from G to $\mathbf{G}_a$ and related results. We fix the notations $G = \mathrm{Spec}\ R$, $\hat{G} = \mathrm{Spec}\ R^*$ as above and we let roman letters $x, y, \ldots$ be elements of R; greek letters $\alpha, \beta, \ldots$ be elements of R^*. Let s and s^* be the co-multiplications in R and R^* respectively. We recall that in §11, we saw how R^* operated naturally on the sheaf $\mathcal{O}_G$. In our affine case, this means that there is a natural inclusion

$$R^* \hookrightarrow \mathrm{Hom}_k(R, R).$$

Explicitly, if $\alpha: R \to k$ is an element of R^*, we get a map $D_\alpha: R \to R$ by the composition

$$R \xrightarrow{s} R \otimes_k R \xrightarrow{1 \otimes \alpha} R.$$

In particular, if $\alpha(1) = 0$, $\alpha(\mathfrak{M}_e^2) = (0)$, then D_α is derivation of R over k. The operators D_α are all translation-invariant in the usual sense. Moreover the transposed maps $D_\alpha^*: R^* \to R^*$ are just the compositions

$$\beta \otimes \alpha \longmapsto \beta$$

$$R^* \xleftarrow{\text{mult.}} R^* \otimes_k R^* \longleftarrow R^*$$

i.e. the maps $\beta \longmapsto \alpha.\beta$, multiplication by α.

As an application, we can interpret $\mathrm{Hom}(\hat{G}, \mathbf{G}_a)$ in a new way:

$$\mathrm{Hom}_{\text{Gp.Sch.}}(\hat{G}, \mathbf{G}_a) \simeq \mathrm{Hom}_{\text{bi-algebra}}(k[X], R^*)$$
$$\simeq \{\alpha \in R^* \mid s^*\alpha = \alpha \otimes 1 + 1 \otimes \alpha\}$$

(since a homomorphism ϕ from $k[X]$ to R^* is determined by the image $\alpha = \phi(X)$, and ϕ is compatible with co-multiplication if and only if $s^*\alpha = \alpha \otimes 1 + 1 \otimes \alpha$). Such α's are called *primitive* elements of R^*. If we associate to any $\alpha \in R^*$ the map D_α which is the transpose of multiplication by α, we see that primitive elements correspond precisely to invariant derivations of R:

$$\left\{\alpha \in R^* \,\middle|\, s^*\alpha = \alpha \otimes 1 + 1 \otimes \alpha\right\} \simeq \left\{D: R \longrightarrow R \,\middle|\, D \text{ an invariant derivation}\right\}$$
$$\simeq \mathrm{Lie}(G).$$

The conclusion is that

$$\mathrm{Hom}(\hat{G}, \mathbf{G}_a) \simeq \mathrm{Lie}(G).$$

Moreover, the p^{th} power operation in $\mathrm{Lie}(G)$ is obtained by taking D to $\overbrace{D \circ \ldots \circ D}^{p\text{x}}$, which corresponds to raising α to its p^{th} power, which corresponds to composing a map $\phi: \hat{G} \to \mathbf{G}_a$ with the Frobenius $F: \mathbf{G}_a \to \mathbf{G}_a$ (since $F^*(X) = X^p$).

Now look at the following type of group.

DEFINITION. *A group scheme G is of height one if it consists of a single point e, and if $x^p = 0$, for all $x \in \mathfrak{M}_e$. (G need not be commutative.)*

It is easy to see that, *as schemes*, such groups G are isomorphic to $\mathrm{Spec}(k[X_1, \ldots, X_n]/(X_1^p, \ldots, X_n^p))$. In fact, choosing $X_1, \ldots, X_n \in \mathfrak{M}_e$ which induce a basis of $\mathfrak{M}_e/\mathfrak{M}_e^2$, and letting $R = \Gamma(\mathcal{O}_G)$, we find that R is a quotient of $k[X_1, \ldots, X_n]/(X_1^p, \ldots, X_n^p)$. On the other hand, if we use the fact that R admits derivations $D_i: R \to R$ such that $D_i(X_j) \equiv \delta_{ij} \pmod{\mathfrak{M}_e}$, then it is easy to see that there can be no relation of linear dependence over k among the monomials

$$\prod_{i=1}^{n} X_i^{a_i},\ 0 \leqslant a_i < p.$$

We have already seen in §11 that any group scheme G has a maximal subgroup scheme $G^{(p)} \subset G$ of height one, having the same Lie algebra as G. Then the analog in characteristic $p > 0$ of the classical equivalence of categories between Lie algebras and germs of Lie groups is the following

THEOREM. *The functor $G \longmapsto \mathrm{Lie}\ G$ sets up an equivalence of the categories of finite group schemes of height one and finite-dimensional p-Lie algebras over k (i.e. a finite-dimensional vector space with bracket and p^{th} power map, as in* §11).

We shall prove this only for commutative G, which correspond to p-Lie algebras with trivial bracket.

PROOF. For any k-vector space $\mathfrak{g}$ with a p-linear map $\alpha \to \alpha^{(p)}$, let $U(\mathfrak{g})$ be the k-algebra $S(\mathfrak{g})/I$, where I is the ideal generated in the symmetric algebra $S(\mathfrak{g})$ of $\mathfrak{g}$ by elements of the form $\alpha^{(p)} - \alpha^p, \alpha \in \mathfrak{g}$. Note that if $\alpha_1, \ldots, \alpha_n$ are a basis of $\mathfrak{g}$, then $\prod_{i=1}^{n} \alpha_i^{r_i}, 0 \leqslant r_i < p$ are a basis of $U(\mathfrak{g})$. Define a co-multiplication $s: U(\mathfrak{g}) \to U(\mathfrak{g}) \otimes_k U(\mathfrak{g})$ by putting for $\alpha \in \mathfrak{g}$, $s\alpha = 1 \otimes \alpha + \alpha \otimes 1$ (check that this goes down to $U(\mathfrak{g})$). It is easily verified that $U(\mathfrak{g})$ is a commutative finite-dimensional bialgebra, and is a covariant functor in $\mathfrak{g}$.

Put $R(\mathfrak{g}) = U(\mathfrak{g})^*$, and $G(\mathfrak{g}) = \mathrm{Spec} U(\mathfrak{g})^*$, considered as a group scheme.

We shall prove that the two functors

$$G \longmapsto \mathrm{Lie}\ G$$

$$\mathfrak{g} \longmapsto G(\mathfrak{g})$$

are inverses of each other.

We prove first that for any vector space $\mathfrak{g}$ with a p-linear map, $G(\mathfrak{g})$ is of height one and there is a natural isomorphism $\mathfrak{g} \xrightarrow{\approx} \mathrm{Lie}\, G(\mathfrak{g})$. Now, we have a natural inclusion $\mathfrak{g} \hookrightarrow U(\mathfrak{g})$ of $\mathfrak{g}$ into the primitive elements of $U(\mathfrak{g})$, which gives an injection $\mathfrak{g} \hookrightarrow \mathrm{Lie}\, G(\mathfrak{g})$. To show that $G(\mathfrak{g})$ is of height one, it suffices to show that for $x \in R(\mathfrak{g})$ belonging to the maximal ideal of 0 in $G(\mathfrak{g})$, $x^p = 0$. If we identify $U(\mathfrak{g})$ with a subalgebra of $\mathrm{End}_k R(\mathfrak{g})$ via D, it will suffice to show that if $\alpha \in U(\mathfrak{g})$, $D_\alpha(x^p) = 0$. Since $U(\mathfrak{g})$ is generated by $\mathfrak{g}$, it even suffices to show that for $\alpha \in \mathfrak{g}$, $D_\alpha(x^p) = 0$, which is clear since D_α is a derivation. It only remains to show that $\mathfrak{g} \to \mathrm{Lie}\, G(\mathfrak{g})$ is surjective. But if $n = \dim_k(\mathfrak{g})$, $m = \dim_k \mathrm{Lie}\, G(\mathfrak{g})$, then by our remarks on a basis of $U(\mathfrak{g})$, $p^n = \dim_k U(\mathfrak{g})$, and by our remarks on the structure of $\Gamma(\mathcal{O}_{G(\mathfrak{g})})$, $p^m = \dim_k R(\mathfrak{g})$. Thus $n = m$, so $\mathfrak{g} \xrightarrow{\sim} \mathrm{Lie}\, G(\mathfrak{g})$.

Secondly, let G be a commutative group scheme of height one with coordinate ring R. Let ϕ: $\mathrm{Lie}(G) \to R^*$ be the usual inclusion map. We have seen in §11 that $\phi(\alpha^{(p)}) = \phi(\alpha)^p$, so ϕ extends to a homomorphism

$$\tilde{\phi}\colon U(\mathrm{Lie}\ G) \longrightarrow R^*.$$

Since for $\alpha \in \mathrm{Lie}\,(G)$, α and $\phi(\alpha)$ are primitive with respect to the co-multiplication in $U(\mathrm{Lie}\, G)$ and R^* resp., $\tilde{\phi}$ is a homomorphism of bi-algebras. The transpose of $\tilde{\phi}$ is again a homomorphism of bi-algebras

$$\tilde{\phi}^*\colon R \longrightarrow R(\mathrm{Lie}\ G)$$

and passing to the Spec's, we obtain a homomorphism of group schemes:

$$\phi'\colon G(\mathrm{Lie}\ G) \longrightarrow G.$$

By the first part of the proof, Lie G is the Lie algebra of $G(\mathrm{Lie}\ G)$ and it follows from our construction that the differential of ϕ' induces an isomorphism from the Lie algebra of $G(\mathrm{Lie}\ G)$ to that of G. Now by Nakayama's lemma, any morphism $f\colon X \to Y$ of schemes with one point each, whose differential is injective, is a closed immersion. This applies to ϕ'; in other words, $\tilde{\phi}^*$ is surjective. But if $n = \dim_k \mathrm{Lie}\ G$, then $p^n = \dim_k R = \dim_k R(\mathrm{Lie}\ G)$. Therefore $\tilde{\phi}^*$ and ϕ' are both isomorphisms.

COROLLARY. *If G is a commutative group scheme of height one, the homomorphism p_G (mult. by p in G) is zero.*

PROOF. In fact, multiplication by p kills Lie G, so the result follows from the Theorem.

If $G = \mathrm{Spec}\ R$ is a group scheme of height one, then not only is its structure as a group determined by its p-Lie algebra but also to give an action of G on a scheme X is equivalent to giving an action of Lie G on X, i.e. a k-linear map $\alpha \longmapsto D_\alpha$ from Lie G to derivations $D_\alpha : \mathcal{O}_X \to \mathcal{O}_X$ such that

(i) $[D_\alpha, D_\beta] = 0$, all $\alpha, \beta \in \mathrm{Lie}\ G$,

(ii) $D_{\alpha(p)} = (D_\alpha)^p$, all $\alpha \in \mathrm{Lie}\ G$.

We can see this in several steps.

(I) To give a map $\alpha \longmapsto D_\alpha$ as above is equivalent to giving a homomorphism of algebras:

$$D\colon U(\mathrm{Lie}\ G) \longrightarrow \mathrm{Diff}(\mathcal{O}_X),$$

where $\mathrm{Diff}(\mathcal{O}_X)$ is the algebra of differential operators on $\mathcal{O}_X$, such that D carries Lie G into derivations.

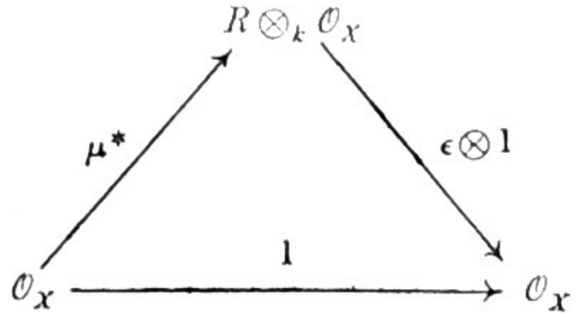
(II) Interpreting D as a map

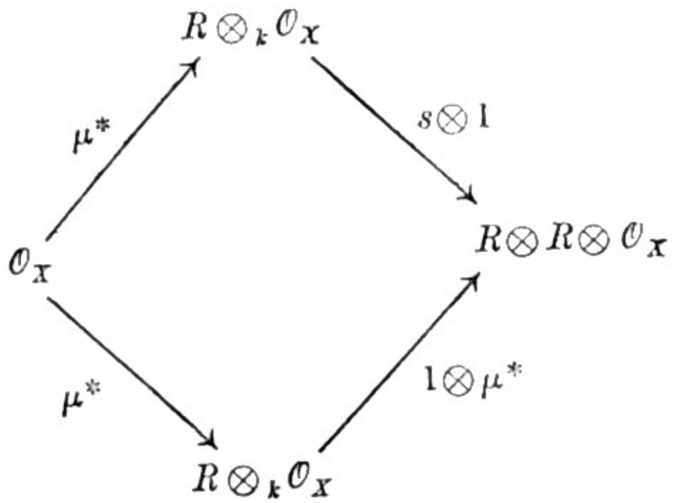
$$\tilde{D}\colon U(\mathrm{Lie}\ G) \otimes_k \mathcal{O}_X \longrightarrow \mathcal{O}_X,$$

and using the fact that the coordinate ring R is the dual of $U(\mathrm{Lie}\ G)$, we see that to give $\widetilde{D}$ is equivalent to giving a transposed map

$$\mu^* : \mathcal{O}_X \longrightarrow R \otimes_k \mathcal{O}_X.$$

The condition that $D(1) = 1$ and $D_{\alpha\beta} = D_\alpha \circ D_\beta$ translate easily into the conditions that





commute. It can also be checked that the condition that D take Lie G to derivations, i.e. D commutes with co-multiplication, means that μ^* is a homomorphism of algebras.

(III) To give a homomorphism μ^* is the same as giving a morphism $\mu: G \times X \to X$ and the two commutative diagrams with μ^* say exactly that μ is an action of G on X.

Finally, let us look at the decomposition into pieces of a commutative finite group scheme G of height one. We get

(*) $$G = G_{l,r} \times G_{l,l}$$

and both $G_{l,r}$ and $G_{l,l}$ are again of height one. Since $G_{l,r}$ is killed by p,

$$G_{l,r} \simeq \mu_p^n$$

for some n. We have seen that Lie (μ_p) is one-dimensional with a generator e such that $e^{(p)} = e$. Now the decomposition (*) induces a decomposition

(**) $$\mathrm{Lie}\ G = \mathrm{Lie}\ G_{l,r} \oplus \mathrm{Lie}\ G_{l,l} = \mathfrak{g}_1 \oplus \mathfrak{g}_2.$$

It follows that $\mathfrak{g}_1$ has a basis $e_1, \ldots, e_n$ such that $e_i^{(p)} = e_i$. On the other hand, since $\widehat{G}_{l,l}$ is again local, and $\mathfrak{g}_2$ is contained in the maximal ideal of $\Gamma(\mathcal{O}_{\widehat{G}_{l,l}})$, it follows that for all $\alpha \in \mathfrak{g}_2$, $\alpha^{(p^n)} = 0$ for n large. In view of the theorem, we deduce a corollary in "p-linear" algebra:

COROLLARY. *If V is any vector space with a p-linear map $x \longmapsto x^{(p)}$, there is a unique decomposition, invariant under $x \longmapsto x^{(p)}$:*

$$V = V_s \oplus V_n,$$

such that V_s has a basis $x_1, \ldots, x_k$ for which $x_i^{(p)} = x_i$, and such that $x \to x^{(p)}$ is a nilpotent map on V_n.

V_s and V_n are called the semi-simple and nilpotent subspaces of V respectively, and in the case of Lie G, *we have:*

$$(\mathrm{Lie}\ G)_s = \mathrm{Lie}\ G_{l,r}$$
$$(\mathrm{Lie}\ G)_n = \mathrm{Lie}\ G_{l,l}.$$

15. Applications to Abelian Varieties.

THEOREM 1. *Let f: $X \to Y$ be an isogeny of abelian varieties, with kernel K. Let $\widehat{f}$: $\widehat{Y} \to \widehat{X}$ be the dual map, with kernel K'. Then there is a canonical isomorphism of K' with the dual $\widehat{K}$ of K.*

PROOF. If L is any line bundle on Y and $x \in X$, then $\phi_{f^*L}(x) \in \widehat{X}$ represents the line bundle $T_x^*(f^*L) \otimes f^*L^{-1}$, and since

$$T_x^*(f^*L) \otimes (f^*L)^{-1} \simeq f^*[T_{fx}^* L \otimes L^{-1}]$$

it follows that

$$\phi_{f^*L}(x) = \widehat{f}(\phi_L(f(x))).$$

In particular, if ϕ_{f^*L} is the zero map, then ϕ_L must be the zero map too; i.e. $f^*L \in \mathrm{Pic}^0 Y \Rightarrow L \in \mathrm{Pic}^0 X$. It follows then that for any scheme S, we have natural isomorphisms:

$$\underline{K}'(S) \simeq \mathrm{Ker}\,[\mathrm{Hom}\,(S, \widehat{Y}) \to \mathrm{Hom}\,(S, \widehat{X})]$$

$$\simeq \mathrm{Ker}\left\{\left[\begin{array}{l}\text{line bundles on}\\ S\times Y\text{, trivial on}\\ S\times(0)\end{array}\right] \longrightarrow \left[\begin{array}{l}\text{line bundles on}\\ S\times X\text{, trivial on}\\ S\times(0)\end{array}\right]\right\}$$

$$\simeq \mathrm{Ker}\left[\left(\begin{array}{l}\text{line bundles on}\\ S\times Y\end{array}\right) \longrightarrow \left(\begin{array}{l}\text{line bundles on}\\ S\times X\end{array}\right)\right].$$

The last isomorphism is correct because if a line bundle on $S\times Y$ becomes trivial on $S\times X$, then it must also be trivial on $S\times(0)$. But now $S\times Y$ is the quotient of $S\times X$ for the free action of K. Thus according to the results in §12, there is a natural isomorphism:

$$\mathrm{Ker}\left[\left(\begin{array}{l}\text{line bundles}\\ \text{on } S\times Y\end{array}\right) \longrightarrow \left(\begin{array}{l}\text{line bundles}\\ \text{on } S\times X\end{array}\right)\right] \simeq \left[\begin{array}{l}\text{Liftings of the}\\ \text{action of } K \text{ on}\\ S\times X \text{ to actions}\\ \text{on } S\times X\times \mathbf{A}^1\end{array}\right].$$

Now an action of K on $S\times X\times \mathbf{A}^1$ is defined by a morphism μ fitting into a diagram:

$$\begin{array}{ccc} K\times S\times X\times \mathbf{A}^1 & \xrightarrow{\ \mu\ } & S\times X\times \mathbf{A}^1 \\ \Big\downarrow{\scriptstyle p_{123}} & & \Big\downarrow{\scriptstyle p_{12}} \\ K\times S\times X & \xrightarrow{\ \mu_0\ } & S\times X \end{array}$$

where μ_0 is the translation action of K on X, with S thrown in. If $\lambda = p_3\circ\mu$ is the induced morphism from $K\times S\times X\times \mathbf{A}^1$ to $\mathbf{A}^1$, then in terms of T-valued points, the lifted action can be described as

$$k\colon (s, x, \alpha) \longmapsto (s, x+k, \lambda(k, s, x, \alpha)),$$

$k\in \underline{K}(T)$, $s\in \underline{S}(T)$, $x\in \underline{X}(T)$, $\alpha\in \underline{\mathbf{A}}^1(T)$. Since the action should be *linear* on $\mathbf{A}^1$,

$$\lambda(k, s, x, \alpha) = \alpha.\lambda(k, s, x, 1).$$

Since X is a complete variety, for any scheme W, $\Gamma(\mathcal{O}_{W\times X})\simeq\Gamma(\mathcal{O}_W)$, hence all morphisms $W\times X\to \mathbf{A}^1$ factor through W. In particular, λ does not depend on the factor x in X. Thus the action is given by

$$k : (s, x, \alpha) \longmapsto (s, x+k, \lambda(k, s, 0, 1).\alpha).$$

To be an action, we need

$$\lambda(k_1+k_2, s, 0, 1) = \lambda(k_1, s, 0, 1).\lambda(k_2, s, 0, 1)$$

$$\lambda(0, s, 0, 1) = 1.$$

In other words, λ is given by an S-homomorphism $\chi\colon K\times S\to \mathbf{G}_m$. Conversely, any such χ defines an action μ via

$$\mu(k, s, x, \alpha) = (s, x+k, \chi(k, s).\alpha).$$

Therefore,

$$\left[\begin{array}{l}\text{Liftings of the action of } K \text{ on } S\times X\\ \text{to actions on } S\times X\times \mathbf{A}^1\end{array}\right] \simeq \mathrm{Hom}_S(K, \mathbf{G}_m) \simeq \underline{\widehat{K}}(S).$$

Putting all this together, $K' \simeq \widehat{K}$.

DEFINITION. *An isogeny $f: X\to Y$ of abelian varieties is said to be of height one if, denoting by $k(Y)$ and $k(X)$ the respective function fields, we have $k(X)^p\subset k(Y)$.*

We shall show that f is of height one if and only if $\ker f$ is a group scheme of height one. In fact, assume f is of height one. $\mathcal{O}_{X,0}$ is the integral closure of $\mathcal{O}_{Y,0}$ in $k(X)$ and $\mathcal{O}_{Y,0}$ is integrally closed. Therefore $\mathcal{O}_{Y,0} = \mathcal{O}_{X,0}\cap k(Y) \supset \{f^p \mid f\in\mathcal{O}_{X,0}\}$, hence $\mathfrak{M}_{Y,0}\supset\{f^p \mid f\in \mathfrak{M}_{X,0}\}$. Since $\ker f \simeq \mathrm{Spec}\,(\mathcal{O}_{X,0}/\mathfrak{M}_{Y,0}.\mathcal{O}_{X,0})$, this shows that $\ker f$ is of height one. Conversely, suppose $K=\ker f$ is of height one, and let R^* be the bialgebra of $\widehat{K}$. Let U be any non-void affine open subset of X with coordinate ring A. The action of K on U is given by a homomorphism of R^* into the algebra of differential operators on A, such that a set of generators of R^* gets mapped into vector fields on U. The elements of A invariant under the

action of K therefore consist precisely of those elements of A which are killed by these derivations; in particular they contain $A^{(p)} = \{f^p \mid f \in A\}$. This proves that $k(X)^p \subset k(Y)$.

THEOREM 2. *For all abelian varieties X, there is a one-one correspondence between isogenies $f: X \to Y$ of height one (up to isomorphism) and sub p-Lie algebras of* Lie X.

PROOF. In fact, isogenies of height one are uniquely determined up to an isomorphism by their kernels, which are subgroup-schemes of height one, or what is the same, subgroup-schemes of the maximal height one subgroup-scheme $X_p = \mathrm{Spec}(\mathcal{O}_{X,0}/\mathfrak{M}_{X,0}^{(p)})$. But by an earlier theorem, subgroup-schemes of X_p are in natural one-one correspondence with p-Lie subalgebras of Lie $X_p = \mathrm{Lie}\, X$.

EXAMPLE. The above theorem enables us to give an example of an abelian variety X admitting an infinity of distinct isogenies $X \to Y$ of height one.

In fact, for every prime $p > 0$, there is an elliptic curve E, unique up to isogeny, such that the p^{th} power map in Lie X is 0 (Deuring; cf. §21). But if E is such a curve, and $X = E \times E$, any 1-dimensional subspace of Lie X is stable for the p^{th} power map, and hence defines an isogeny of height one.

THE p-RANK.

Let X be an abelian variety of dimension g in characteristic $p > 0$, and $n = p^r \cdot m$ an integer > 0, $r \geqslant 0$, $m \geqslant 1$, $(p, m) = 1$. We want to analyze the structure of the finite group *scheme* $X_n = \ker n_X$. Now, X_m and X_{p^r} are subgroup schemes of X_n, and we have a homomorphism $X_m \times X_{p^r} \to X_n$. This is, in fact, an isomorphism since X_m is the (r, r)-part of X_n, and X_{p^r} is the product of the (r, l), (l, r) and (l, l)-parts of X_n. As we saw in §6, X_m is a discrete reduced group isomorphic to $(\mathbf{Z}/m\mathbf{Z})^{2g}$. Thus, it suffices to study the structure of X_{p^n}, which we rename G_n. Suppose now that $(G_1)_{\text{red}} = (\mathbf{Z}/p\mathbf{Z})^r$. Since X is divisible, for any $n \geqslant 1$, we have an exact sequence $0 \to G_{1,\text{red}} \to G_{n+1,\text{red}} \xrightarrow{p} G_{n,\text{red}} \to 0$,

and one deduces by induction that for any $n \geqslant 1$, $(G_n)_{\text{red}} = (\mathbf{Z}/p^n\mathbf{Z})^r$. Now, by Theorem 1 of this section, $\hat{G}_n$ is the kernel of $(p^n)_{\hat{X}}$, so it follows that there is an integer s such that for any $n \geqslant 0$, $(\hat{G}_n)_{\text{red}} = (\mathbf{Z}/p^n\mathbf{Z})^s$. Thus, the decomposition of G_n into its pieces is as follows:

$$G_n = (\mathbf{Z}/p^n\,\mathbf{Z})^r \times (\mathbf{Z}/\widehat{p^n\mathbf{Z}})^s \times G_n^0$$

$$= (\mathbf{Z}/p^n\,\mathbf{Z})^r \times \mu_{p^n}^s \times G_n^0,$$

where G_n^0 is local-local. Since G_n is of order p^{2ng}, we deduce that there is an integer $t \geqslant 0$ such that $r + s + t = 2g$, and G_n^0 is of order p^{nt}.

We shall show that the integers $r = r_X$, $s = s_X$ and $t = t_X$ are the same for isogenous abelian varieties. It suffices to prove this for r and s, since $r+s+t=2g$. Further, since $s_X = r_{\hat{X}}$, it even suffices to verify this for r. Let $f: X \to Y$ be an isogeny, with kernel of order k. Since $f(X_{p^n}) \subseteq Y_{p^n}$, we have that the order of $(X_{p^n})_{\text{red}}$ is at most k times that of $(Y^{p^n})_{\text{red}}$, that is, $p^{nr_X} \leqslant k \cdot p^{nr_Y}$ for all n, hence $r_X \leqslant r_Y$. Now, $\ker f$ is a finite group scheme, hence is annihilated by an $N > 0$, which shows that $\ker N_X \supset \ker f$. Therefore, N_X factorizes as $X \xrightarrow{f} Y \xrightarrow{g} X$. Thus, $Y \xrightarrow{g} X$ is an isogeny, and $r_Y \leqslant r_X$. This proves that r, s and t are isogeny invariant. In particular, since for any abelian variety X, X and $\hat{X}$ are isogenous, we deduce that $r_X = r_{\hat{X}} = s_X$. Thus, we have that

$$G_n = (\mathbf{Z}/p^n\mathbf{Z})^r \times (\mu_{p^n})^r \times G_n^0$$

with G_n^0 local-local of order p^{nt}, $2r + t = 2g$. In particular, we see that $r \leqslant g$. The integer r is called the *p-rank* of X, and is an isogeny invariant.

Now, since p_X induces the 0-map on Lie algebras, we see that Lie $X = \mathrm{Lie}\,(\ker p_X) = \mathrm{Lie}\, G_1 = \mathrm{Lie}\,(\mu_p)^r \oplus \mathrm{Lie}\, G_1^0$. Since G_1^0 is local-local, the p^{th} power map on $\mathrm{Lie}\, G_1^0$ is nilpotent, whereas $\mathrm{Lie}(\mu_p)^r$ admits a basis $e_1, \ldots, e_r$ such that $e_i^p = e_i$. We thus see

that the p-rank of X equals the dimension of the semi-simple part of Lie X with respect to the p^{th} power map. The same result holds for Lie $\hat{X}$, since X and $\hat{X}$ have the same p-rank. On the other hand, we have established a canonical isomorphism Lie $\hat{X} \simeq H^1(X, \mathcal{O}_X)$. Let $F: \mathcal{O}_X \to \mathcal{O}_X$ be the Frobenius homomorphism $F(\alpha) = \alpha^p$, and denote the induced p-linear map $H^1(X, \mathcal{O}_X) \to H^1(X, \mathcal{O}_X)$ again by F. We shall establish that under the isomorphism Lie $\hat{X} \simeq H^1(X, \mathcal{O}_X)$, the p^{th} power map in Lie X goes over into F. It follows that the p-rank of X is also the dimension of the semi-simple part of $H^1(X, \mathcal{O}_X)$ with respect to the Frobenius map F. Thus, we need to prove

THEOREM 3. *Under the natural isomorphism* Lie $\hat{X} \simeq H^1(X, \mathcal{O}_X)$, *the p^{th} power operation in* Lie $\hat{X}$ *goes over into the Frobenius map in* $H^1(X, \mathcal{O}_X)$.

PROOF. First we give a description of the p^{th} power operation on vector fields on a scheme X, using the functor $\underline{X}$, analogous to the one given for the Poisson bracket in §11. Let D be a vector field, interpreted now as an automorphism of $X \times \operatorname{Spec} \Lambda$ over $\operatorname{Spec} \Lambda$, where $\Lambda = \dfrac{k[\epsilon]}{(\epsilon^2)}$, which is the identity on the closed fibre $X \hookrightarrow X \times \operatorname{Spec} \Lambda$.

Let $M = k[\epsilon_1, \ldots, \epsilon_p]/(\epsilon_1^2, \ldots, \epsilon_p^2)$, and let $\eta_i : \Lambda \to M$ be the k-algebra homomorphisms defined by $\eta_i(\epsilon) = \epsilon_i$ and let $\phi_i = \operatorname{Spec} \eta_i$: $\operatorname{Spec} M \to \operatorname{Spec} \Lambda$. By base change using ϕ_i, D induces an automorphism D_i of $X \times \operatorname{Spec} M$ over $\operatorname{Spec} M$, and hence $D' = D_1 \circ D_2 \circ \ldots \circ D_p$ is an automorphism of $X \times \operatorname{Spec} M$ over $\operatorname{Spec} M$. Let s_i $(1 \leqslant i \leqslant p)$ be the elementary symmetric functions in M of degree i in $\epsilon_1, \ldots, \epsilon_p$. One checks trivially that $s_1 s_i = (i+1)s_{i+1}$ $(1 \leqslant i \leqslant p-1)$, so that the subring M' in M generated by $s_1, \ldots, s_p$ is $k[s_1, s_p]$. Let $\psi : \operatorname{Spec} M \to \operatorname{Spec} M'$ be the natural morphism. We then assert that there is a unique automorphism D'' of $X \times \operatorname{Spec} M'$ over $\operatorname{Spec} M'$ which induces D' on base extension to $\operatorname{Spec} M$. Further, the only relations between s_1, s_p in $M' = k[s_1, s_p]$ are $s_1^p = 0$, $s_p^2 = 0$, so that we have a homomorphism $\eta : M' \to \Lambda$, $\eta(s_1) = 0$, $\eta(s_p) = \epsilon$. Let $\phi = \operatorname{Spec} \eta : \operatorname{Spec} \Lambda \to \operatorname{Spec} M'$. We have defined the maps

$$\Lambda \xrightarrow{\eta_i} M \supset M' \xrightarrow{\eta} \Lambda$$

$$\operatorname{Spec} \Lambda \xleftarrow{\phi_i} \operatorname{Spec} M \xrightarrow{\psi} \operatorname{Spec} M' \xleftarrow{\phi} \operatorname{Spec} \Lambda.$$

Then via ϕ, D'' induces an automorphism D''' of $X \times \operatorname{Spec} \Lambda$ over $\operatorname{Spec} \Lambda$ which on the closed fibre $X \hookrightarrow X \times \operatorname{Spec} \Lambda$ is the identity. So D''' may be thought of as a vector field on X. We assert that $D''' = D^{(p)}$.

To verify these assertions, we may assume $X = \operatorname{Spec} A$. Then D_i is obtained by the automorphism of M-algebras $A \otimes_k M \to A \otimes_k M$ determined by $a \longmapsto a + (Da) \cdot \epsilon_i$, and D' by the automorphism of $A \otimes_k M$ over M determined by

$$a \longmapsto \left\{ \prod_i (1 + \epsilon_i D) \right\} a = (1 + s_1 D + s_2 D^2 + \ldots + s_p D^p) a.$$

Our assertions can be read off from this.

Now suppose G is a group scheme and D a left invariant vector field, whose value at the identity is the tangent vector $t \in \underline{G}(\Lambda)$. Then the corresponding automorphism of $G \times \operatorname{Spec} \Lambda$ is just translation by t, and D_i is translation of $G \times \operatorname{Spec} M$ by the image of t under the morphism $\underline{G}(\Lambda) \xrightarrow{\underline{G}(\eta_i)} \underline{G}(M)$. Hence D' is translation by $t' = \prod_{i=1}^{p} \underline{G}(\eta_i)\,(t) \in G(M)$. Now, t' is the image of an element $t'' \in \underline{G}(M')$ by the map $\underline{G}(M') \to \underline{G}(M)$. The homomorphism $\underline{G}(M)$: $\underline{G}(M') \to \underline{G}(\Lambda)$ maps t'' to $t^{(p)}$.

$$\begin{array}{ccccccc} t & & t' & & t' & & t^{(p)} \\ \in & & \in & & \in & & \in \\ \underline{G}(\Lambda) & \longrightarrow & \underline{G}(M) & \longleftarrow & G(M') & \longrightarrow & \underline{G}(\Lambda). \end{array}$$

Apply these remarks to the situation where X is an abelian variety and $\hat{X}$ its dual, with $G = \hat{X}$. Then for any k-algebra R, $\underline{G}(R)$ is the group of all line bundles L on $X \times \operatorname{Spec} R$ trivial on

$\{0\} \times \operatorname{Spec} R$ such that for any point $P \in \operatorname{Spec} R$, $L|X \times \{P\}$ belongs to $\operatorname{Pic}^0 X$. One sees by definition that if the 1-cocycle $\{f_{ij}\}$ for a covering $\mathfrak{U}$ of X with coefficients in the sheaf $\mathcal{O}_X$ represent a cohomology class ξ in $H^1(X, \mathcal{O}_X)$, the corresponding tangent vector $t_\xi \in \operatorname{Lie} \hat{X} \subset \underline{\hat{X}}(\Lambda) \simeq H^1(X, \mathcal{O}^*_{X \times \operatorname{Spec} \Lambda})$ is represented by the 1-cocycle $\{1 + \epsilon f_{ij}\}$ for the same covering. Hence, the element of $\underline{\hat{X}}(M) \subset H^1(X, \mathcal{O}^*_{X \times \operatorname{Spec} M})$ we obtain is represented by the 1-cocycle $\prod_{r=1}^{p} (1 + \epsilon_r f_{ij}) = (1 + f_{ij} s_1 + f_{ij}^2 s_2 + \ldots + f_{ij}^p s_p)$. It follows that $t_\xi^{(p)} \in \operatorname{Lie} \hat{X} \subset \underline{\hat{X}}(\Lambda)$ is represented by the 1-cocycle $\{1 + f_{ij}^p \epsilon\}$, and hence comes from the 1-cocycle $\{f_{ij}^p\}$ for $\mathcal{O}_X$.

16. Cohomology of Line Bundles. Our first aim in this section is to prove the two following theorems.

THE RIEMANN-ROCH THEOREM. *For all line bundles L on X, if $L \simeq \mathcal{O}_X(D)$, we have*

$$\chi(L) = \frac{(D^g)}{g!},$$

$$\chi(L)^2 = \deg \phi_L,$$

where (D^g) is the g-fold self-intersection number of D.

THE VANISHING THEOREM. *If for a line bundle L on X, $K(L)$ is finite, there is a unique integer $i = i(L)$, $0 \leqslant i(L) \leqslant g$, such that $H^p(X, L) = (0)$ for $p \neq i$ and $H^i(X, L) \neq (0)$. Further, $i(L^{-1}) = g - i(L)$.*

PROOFS. (1) If L_1 and L_2 are two line bundles on X such that $L_1 \otimes L_2^{-1} \in \operatorname{Pic}^0 X$, then $\chi(L_1) = \chi(L_2)$. In fact consider the line bundle $p_1^*(L_1) \otimes P$ on $X \times \hat{X}$. Then the Euler characteristic of its restriction L_y to $X \times \{y\}$, $(y \in \hat{X})$, is independent of y. But L_1 and L_2 are both isomorphic to one of the L_y's, so $\chi(L_1) = \chi(L_2)$. Next, if L is symmetric, $n_X^*(L^m) \simeq L^{mn^2}$, so

$$\chi(L^{mn^2}) = \chi(n_X^* L^m) = \deg n_X \cdot \chi(L^m) = n^{2g} \cdot \chi(L^m). \tag{*}$$

Since any L can be written $L_1 \otimes L_2$ where L_1 is symmetric and $L_2 \in \operatorname{Pic}^0 X$, (*) holds for any line bundle L. Since $\chi(L^k)$ is a polynomial in k, (*) shows that $\chi(L^k)$ (for any L) is a homogeneous polynomial of degree g. Let

$$\chi(L^k) = a(L) \cdot \frac{k^g}{g!},$$

so that $\chi(L) = \dfrac{a(L)}{g!}$, and we have only to establish that $a(L) = (D^g)$ if $L = \mathcal{O}(D)$. Assume this for the moment when L is very ample, and let L_i $(i = 1, 2)$ be very ample. Then

$$P(n_1, n_2) = g! \cdot \chi(L_1^{n_1} \otimes L_2^{n_2})$$

is a polynomial in n_1 and n_2. Since $\chi(L_1^{kn_1} \otimes L_2^{kn_2}) = k^g \cdot \chi(L_1^{n_1} \otimes L_2^{n_2})$, P is homogeneous of degree g. If D_i is the divisor corresponding to L_i, since $L_1^{n_1} \otimes L_2^{n_2}$ is very ample for $n_1, n_2 \geqslant 1$, we see that $P(n_1, n_2) = ((n_1 D_1 + n_2 D_2)^g) = \sum_{i=0}^{g} \binom{g}{i} n_1^i n_2^{g-i} (D_1^i D_2^{g-i})$ if $n_1, n_2 \geqslant 1$, and it follows that the same equality holds for all $n_1, n_2 \in \mathbf{Z}$, in particular for $n_1 = 1, n_2 = -1$. But now any line bundle L on X can be written as $L_1 \otimes L_2^{-1}$ with L_i very ample.

Thus, it only remains to show that $a(L) = (D^g)$ for L very ample. We can then choose sections $\sigma_0, \ldots, \sigma_g$ of L on X such that (i) σ_i have no common zero, and (ii) the divisor of zeros of $\sigma_1, \ldots, \sigma_g$ intersect transversally at (D^g) distinct points. Because of condition (i), we get a morphism $X \xrightarrow{\phi} \mathbf{P}^g$ defined by $x \longmapsto (\sigma_0(x), \ldots, \sigma_g(x))$, and by (ii), the 0-cycle $\phi^{-1}((1, 0, \ldots, 0))$ is of degree (D^g), hence ϕ is of degree (D^g). Hence, by the proposition in the appendix to §6, $a(L)$ is (D^g) times the leading coefficient of $g! \chi(\mathcal{O}_{\mathbf{P}^g}(n))$, i.e. $a(L) = (D^g)$.

Next, we have to show that $\chi(L)^2 = \deg \phi_L$. Suppose first that $K(L)$ is finite. Then, by definition of ϕ_L, we have

$$(1_X \times \phi_L)^* P \simeq m^* L \otimes p_1^* L^{-1} \otimes p_2^* L^{-1}$$

on $X \times X$. Arguing as in §8 and §13, we see that $m^* L \otimes p_1^* L^{-1} \otimes p_2^* L^{-1}$ has higher direct images on the first factor concentrated on the finite set $K(L)$. Therefore,

$$R^ip_{1,*}(m^*L\otimes p_1^*L^{-1}\otimes p_2^*L^{-1}) \simeq R^ip_{1,*}(m^*L\otimes p_2^*L^{-1})\otimes L^{-1}$$
$$\simeq R^ip_{1,*}(m^*L\otimes p_2^*L^{-1}).$$

It follows that

$$\chi(m^*L\otimes p_1^*L^{-1}\otimes p_2^*L^{-1}) = \sum_{i=0}^{g}(-1)^i\chi(R^ip_{1,*}(m^*L\otimes p_1^*L^{-1}\otimes p_2^*L^{-1}))$$
$$= \sum_{i=0}^{g}(-1)^i\chi(R^ip_{1,*}(m^*L\otimes p_2^*L^{-1}))$$
$$= \chi(m^*L\otimes p_2^*L^{-1}).$$

Since $(m,p_2): X\times X\to X\times X$ is an isomorphism, and $(m,p_2)^*[p_1^*L\otimes p_2^*L^{-1}]\simeq m^*L\otimes p_2^*L^{-1}$, we find

$$\chi(m^*L\otimes p_2^*L^{-1}) = \chi(p_1^*L\otimes p_2^*L^{-1})$$
$$= \chi(L)\cdot\chi(L^{-1})$$
$$= (-1)^g.\ \chi(L)^2.$$

Since $X\times\hat{X}$ is the quotient of $X\times X$ by the free action of $K(L)$, we deduce that

$$(-1)^g.\deg\phi_L = \deg\phi_L\cdot\chi(P)$$
$$= \chi((1_X\times\phi_L)^*P)$$
$$= \chi(m^*L\otimes p_1^*L^{-1}\otimes p_2^*L^{-1})$$
$$= (-1)^g\cdot\chi(L)^2.$$

Finally suppose $K(L)$ is not finite. We can choose a finite subgroup $F\subset K(L)$ of arbitrarily large order f. The map $1_X\times\phi_L$: $X\times X\to X\times\hat{X}$ therefore factors as $X\times X\to X\times X/F\to X\times\hat{X}$ so that $m^*L\otimes p_2^*L^{-1}$ being the inverse image by $1_X\times\phi_L$ of $P\otimes p_1^*L$, has Euler characteristic divisible by f. Since this holds for arbitrarily large f, $m^*L\otimes p_2^*L^{-1}$ has Euler characteristic 0. But as before $\chi(m^*L\otimes p_2^*L^{-1}) = (-1)^g\chi(L)^2$. So $\chi(L)=0$ and $\deg\phi_L = 0$.

This proves the Riemann-Roch theorem.

(2) We have the Cartesian diagram

$$\begin{array}{ccc} X\times X & \xrightarrow{p_2} & X \\ {\scriptstyle 1\times\phi_L}\downarrow & & \downarrow{\scriptstyle \phi_L} \\ X\times\hat{X} & \xrightarrow{p_2'} & \hat{X} \end{array}$$

(i.e. the left top corner identifies itself to the fibre product of the lower left and upper right corners), and $m^*L\otimes p_1^*L^{-1}\otimes p_2^*L^{-1}$ $\simeq (1\times\phi_L)^*(P)$. Since ϕ_L is flat, we have by Corollary 5, §5, that

$$\phi_L^*(R^qp_{2,*}'(P))\simeq R^qp_{2,*}((1\times\phi_L)^*(P))$$
$$\simeq R^qp_{2,*}(m^*L\otimes p_1^*L^{-1}\otimes p_2^*L^{-1}).$$

But we have seen in §13 that $R^qp_{2,*}'(P)=(0)$ if $q\neq g$ and $R^gp_{2,*}'(P)$ is the residue field $k(0)$ at $0\in\hat{X}$. Hence, we deduce that

$$R^qp_{2,*}(m^*L\otimes p_1^*L^{-1}\otimes p_2^*L^{-1}) = \begin{cases}(0)\text{ if } q\neq g\\ \mathcal{O}_{K(L)}\text{ if } q=g.\end{cases}\qquad(*)$$

Since $K(L)$ is finite, by arguments which we used in (1), we may replace $m^*L\otimes p_1^*L^{-1}\otimes p_2^*L^{-1}$ by $m^*L\otimes p_1^*L^{-1}$ in (*). Taking cohomologies, we get that

$$\dim H^q(X\times X,\ m^*L\otimes p_1^*L^{-1}) = \begin{cases}0\text{ if } q\neq g\\ \deg\phi_L\text{ if } q=g.\end{cases}$$

In this formula, we may as in (1) replace $m^*L\otimes p_1^*L^{-1}$ by $p_2^*L\otimes p_1^*L^{-1}$, so using the Künneth formula, we see that if $h^i(L)=\dim H^i(X,L)$,

$$\sum_{i=0}^{q}h^i(L)\,h^{q-i}(L^{-1}) = \begin{cases}0\text{ if } q\neq g\\ \deg\phi_L\text{ if } q=g.\end{cases}$$

Since all these h^i's are non-negative, it is easy to see that this can only hold if *only one* of the $h^i(L)$'s is positive and *only one* of the $h^i(L^{-1})$'s is positive, and that the sum of these two i's is g.

REMARKS. Consider the case $k = \mathbf{C}$, $X = V/U$ where V is a g-dimensional complex vector space and U a lattice in V. Let $L = L(H, \alpha)$ be a line bundle on X and $E = \operatorname{Im} H$ so that E is a skew symmetric real bilinear form on V and $E(U \times U) \subset \mathbf{Z}$. We consider V as an oriented vector space by means of the complex structure. If $u_1, \ldots, u_{2g}$ is a basis of U, we call $\det(E(u_i, u_j))$ the determinant of E; this is independent of choice of basis for U and is always positive. Further, we have seen that $K(L)$ is finite if and only if E is non-degenerate, and that

$$\deg \phi_L = \text{Order } K(L) = \text{order } (U^\perp/U),$$

where $U^\perp = \{x \in V \mid E(x, u) \in \mathbf{Z}, \forall\ u \in U\}$. Now, the elements λ_i defined by $\lambda_i(x) = E(x, u_i)$ form a basis of the dual, $\operatorname{Hom}(U^\perp, \mathbf{Z})$, of $U^\perp$, so that we have

$$\text{order } (U^\perp/U) = \det(\lambda_i(u_j)) = \det(E(u_i, u_j)).$$

Hence we obtain that $|\chi(L)| = +\sqrt{\det(E(u_i, u_j))}$. Now, given any skew symmetric matrix A of degree $2g$, it is well known that there is a uniquely determined polynomial function $\operatorname{pf}(A)$, the Pfaffian of A, in the entries of A, such that $\operatorname{pf}(A)^2 = \det A$ and $\operatorname{pf}((E_0)) = 1$ where E_0 is the matrix

$$E_0 = \left(\begin{array}{cc|cc|c} 0 & -1 & & & \\ 1 & 0 & \multicolumn{2}{c|}{\mathbf{0}} & \mathbf{0} \\ \hline & & 0 & -1 & \\ \multicolumn{2}{c|}{\mathbf{0}} & 1 & 0 & \mathbf{0} \\ \hline & & & & \ddots \\ \multicolumn{2}{c|}{\mathbf{0}} & \multicolumn{2}{c|}{\mathbf{0}} & \end{array}\right).$$

Now, if X runs through $SL(2g, \mathbf{C})$, $\operatorname{pf}(X'AX)^2 = \det X'AX = \det A = \operatorname{pf}(A)^2$ and since $SL(2g, \mathbf{C})$ is connected, we deduce that $\operatorname{pf}(X'AX) = \operatorname{pf}(A)$ if $X \in SL(2g, \mathbf{C})$. Now, two different bases $u_1, \ldots, u_{2g}$ of U such that $u_1 \wedge \ldots \wedge u_{2g}$ is *positive* differ by a matrix in $SL(2g, \mathbf{R})$, so that for such $u_1, \ldots, u_{2g}$, $\operatorname{pf}(E(u_i, u_j))$ is independent of the choice of basis, i.e. it is determined by E, the lattice U and the orientation of V induced by the complex structure on V. We then assert that we have actually

$$\chi(L) = \operatorname{pf}(E(u_i, u_j)). \qquad (*)$$

Since both sides extend to functions on $\mathbf{Q} \otimes_{\mathbf{Z}} \operatorname{Pic} X$ which on any finite-dimensional subspace is a polynomial function, we see that either $\chi(L) = \operatorname{pf}(E(u_i, u_j))$ for all L or $\chi(L) = -\operatorname{pf}(E(u_i, u_j))$ for all L. If we show that for L ample, $\operatorname{pf}(E(u_i, u_j))$ is positive, it would follow that only the first alternative can hold. But then, $L = L(H, \alpha)$ with H positive definite hermitian. Thus, we have only to show that if H is positive definite hermitian on a complex vector space V and $u_1, u_2, \ldots, u_{2g}$ is any real basis with $u_1 \wedge \ldots \wedge u_{2g}$ positive, $\operatorname{pf}(\operatorname{Im} H(u_i, u_j)) > 0$. By our earlier remark, if this holds for one such basis, it holds for any other such. Thus we may use a $\mathbf{R}$-basis $u_1, iu_1, u_2, iu_2, \ldots, iu_g$ where $H(u_i, u_j) = \delta_{ij}$. But now, the matrix of $\operatorname{Im} H$ with respect to this basis equals E_0 and the Pfaffian of this matrix is 1.

This proves the assertion.

THE INDEX OF LINE BUNDLES.

The purpose of the rest of this section is to prove that $i(L)$ can be computed as follows.

THEOREM. *Let L be an ample line bundle on an abelian variety X, and M a non-degenerate line bundle†. Let $P(t)$ be the polynomial defined by $P(n) = \chi(L^n \otimes M)$. Then P has all its g roots real and the index of M equals the number of positive roots, counted with multiplicity, of $P(t)$.*

The proof will be given in a series of steps. We make heavy use of the next lemma. Before stating the lemma, let us introduce some notations. For $a = (a_1, \ldots, a_k) \in \mathbf{Z}^k$, we write $|a| = \sum_{i=1}^{k} |a_i|$, and if $L_1, \ldots, L_k$ are k-line bundles, we denote the line bundle $L_1^{a_1} \otimes L_2^{a_2} \otimes \ldots \otimes L_k^{a_k}$ by L^a.

† By definition, this means $K(M)$ is finite.

LEMMA. *Let X be a projective variety of dimension r and $L_1, \dots, L_k$ line bundles on X. Then there is a constant c depending only on the L_i such that*

$$\dim H^i(L^a) < c(1 + |a|^r)$$

for $i > 0$ and $a \in \mathbf{Z}^k$.

PROOF. We can easily reduce ourselves to the case when the L_i are all very ample. In fact, choose a very ample L_{k+1} such that $L_i \otimes L_{k+1}$ are very ample for $1 \leqslant i \leqslant k$, and put $L_i' = L_i \otimes L_{k+1}$, $L_{k+1}' = L_{k+1}$. Then there is a linear automorphism T of $\mathbf{Z}^{k+1}$ such that for $a = (a_1, \dots, a_{k+1}) \in \mathbf{Z}^{k+1}$, $L_1^{a_1} \otimes \dots \otimes L_{k+1}^{a_{k+1}} = (L')^{Ta}$ and $\alpha^{-1}|a| \leqslant |Ta| \leqslant \alpha|a|$ for a suitable $\alpha > 0$.

Thus we assume all L_i $(1 \leqslant i \leqslant k)$ very ample. We proceed by induction on the integer $\nu = \dim X + k$. When $\nu = 0$, the assertion is trivial. Thus we may assume $\nu > 0$ and that the assertion holds for smaller values of ν. If now $k = 0$, the assertion is again clear. Thus suppose $k > 0$, and let L' be the system of line bundles $\{L_1, \dots, L_{k-1}\}$ and for $a = (a_1, \dots, a_k) \in \mathbf{Z}^k$, set $a' = (a_1, \dots, a_{k-1}) \in \mathbf{Z}^{k-1}$. Then the existence of a constant c for all $a \in \mathbf{Z}^k$ with $a_k = 0$ follows by induction hypothesis. For any $\mu \in \mathbf{Z}$, we have an exact sequence

$$0 \longrightarrow L'^{a'} \otimes L_k^{\mu} \longrightarrow L'^{a'} \otimes L_k^{\mu+1} \longrightarrow L'^{a'} \otimes L_k^{\mu+1}|_H \longrightarrow 0$$

where H is a hyperplane section for the projective imbedding of X given by L_k. Suppose now that $a_k > 0$. We have the exact sequence

$$H^i(L'^{a'} \otimes L_k^{\mu}) \longrightarrow H^i(L'^{a'} \otimes L_k^{\mu+1}) \longrightarrow H^i(H, L'^{a'} \otimes L_k^{\mu+1}|_H)$$

from which we have

$$\dim H^i(L'^{a'} \otimes L_k^{\mu+1}) - \dim H^i(L'^{a'} \otimes L_k^{\mu}) \leqslant \dim H^i(H, L'^{a'} \otimes L_k^{\mu+1}|_H) \leqslant c(|a|^{r-1} + 1)$$

for $0 \leqslant \mu < a_k$ and a suitable constant c, by induction hypothesis. Summing over all μ with $0 \leqslant \mu < a_k$, we obtain

$$\dim H^i(L'^{a'} \otimes L_k^{a_k}) \leqslant C.|a_k|(|a|^{r-1} + 1) + \dim H^i(L'^{a'}) < C'(|a|^r + 1).$$

Similarly, if $a_k < 0$, the exactness of

$$H^{i-1}(H, L'^{a'} \otimes L_k^{\mu+1}|_H) \longrightarrow H^i(X, L'^{a'} \otimes L_k^{\mu}) \longrightarrow H^i(X, L'^{a'} \otimes L_k^{\mu+1})$$

gives, for $0 > \mu \geqslant a_k$, the inequalities

$$\dim H^i(L'^{a'} \otimes L_k^{\mu}) - \dim H^i(L'^{a'} \otimes L_k^{\mu+1}) \leqslant \dim H^{i-1}(H, L'^{a'} \otimes L_k^{\mu+1}|_H) < C(1 + |a|^{r-1})$$

and summing over μ with $0 > \mu \geqslant a_k$, we get as before the required inequality.

STEP A. Let L be any non-degenerate line bundle on an abelian variety X and H a very ample line bundle on X, and let P be the polynomial in two variables defined by $P(m, n) = \chi(L^m \otimes H^n)$. If $P(1, t) \neq 0$ for $0 < t < 1$, then $i(L) = i(L \otimes H)$.

PROOF. The following remark is essential to what follows. If $f: X \to Y$ is an isogeny of abelian varieties of degree prime to p and L a line bundle on Y with $\chi(L) \neq 0$, $i(f^*(L)) = i(L)$. In fact, we know by Cor. to Prop. 3, §7 that L is a direct summand of $f_*(f^*(L))$, and $H^i(X, f^*(L)) \simeq H^i(Y, f_*(f^*(L)))$, so that $H^i(L) \neq (0) \Rightarrow H^i(f_*(f^*L)) \neq (0) \Rightarrow H^i(f^*(L)) \neq (0)$. Also if $L_0 \in \mathrm{Pic}^0 X$, then $i(L) = i(L \otimes L_0)$. In fact, for some $x \in X$, $L \otimes L_0 \simeq T_x^* L$, hence $H^i(L) \neq (0) \Rightarrow H^i(T_x^* L) \neq (0) \Rightarrow H^i(L \otimes L_0) \neq (0)$. In particular, since $n_X^*(L) = L^{n^2} \otimes L_0$ with $L_0 \in \mathrm{Pic}^0 X$, we see that $i(L^{n^2}) = i(L)$ for any $n > 0$, with $p \nmid n$.

Suppose then that N is a large square prime to p. If $i(L) \neq i(L \otimes H)$, then $i(L^N) \neq i(L^N \otimes H^N)$, so there is a least integer a in $0 < a \leqslant N$ with $i_1 = i(L^N \otimes H^a) \neq i(L^N \otimes H^{a-1}) = i(L^N)$. (Note that since $P(1,t)$ has no rational zeroes, $0 \leqslant t < 1$, all the bundles $L^N \otimes H^a$ are non-degenerate so $i(L^N \otimes H^a)$ is well defined.) The exact sequence $0 \to L^N \otimes H^{a-1} \to L^N \otimes H^a \to L^N \otimes H^a|_V \to 0$, where V is a hyperplane section of X for the imbedding given by H, gives us that

$$0 \longrightarrow H^{i_1}(L^N \otimes H^a) \longrightarrow H^{i_1}(L^N \otimes H^a|_V)$$

is exact so that

$$\dim H^{i_1}(V, L^N \otimes H^a|_V) \geq \dim H^{i_1}(L^N \otimes H^a)$$
$$= |\chi(L^N \otimes H^a)|$$
$$= N^g . P\left(1, \frac{a}{N}\right).$$

But there is a lower bound

$$P(1, t) \geq c > 0 \text{ if } 0 \leq t \leq 1,$$

and since this holds for arbitrarily large N, while V is of dimension $g-1$, we get a contradiction to the lemma.

STEP B. If L_1 and L_2 are two line bundles on an abelian variety and $F(s, t)$ is the homogeneous polynomial defined by $F(m, n) = \chi(L_1^m \otimes L_2^n)$, and if $F(t, 1-t) \neq 0$ for $0 \leq t \leq 1$, then $i(L_1) = i(L_2)$.

PROOF. Choose a very ample L_3 such that $L_1 \otimes L_3 \otimes L_2^{-1}$ is also very ample. Set $f(a, b, c) = \chi(L_1^a \otimes L_2^b \otimes L_3^c)$, so that $f(a, b, 0) = F(a, b)$. Since $F(t, 1-t) \neq 0$ for $0 \leq t \leq 1$, by continuity, we can choose a square N, prime to p, so large that for $0 \leq r \leq N-1$, $0 \leq t \leq 1$,

$$f(N-r, r, t) = N^g f\left(1 - \frac{r}{N}, \frac{r}{N}, \frac{t}{N}\right) \neq 0,$$

$$f(N-r-1+t, r+1-t, t) = N^g f\left(1 - \frac{r+1-t}{N}, \frac{r+1-t}{N}, \frac{t}{N}\right) \neq 0.$$

The first equation coupled with Step A gives us that for $0 \leq r \leq N-1$, r an integer,

$$i(L_1^{N-r} \otimes L_2^r) = i(L_1^{N-r} \otimes L_2^r \otimes L_3)$$

and the second gives us that

$$i(L_1^{N-r} \otimes L_2^r \otimes L_3) = i(L_1^{N-r-1} \otimes L_2^{r+1})$$

for $0 \leq r \leq N-1$, r an integer. Taken together, we get that for r in the same range,

$$i(L_1^{N-r} \otimes L_2^r) = i(L_1^{N-r-1} \otimes L_2^{r+1}),$$

so that we obtain

$$i(L_1) = i(L_1^N) = i(L_2^N) = i(L_2).$$

COROLLARY. *If L is non-degenerate and n any integer > 0,*

$$i(L) = i(L^n).$$

STEP C. If L_1, L_2, and $L_1 \otimes L_2$ are non-degenerate,

$$i(L_1 \otimes L_2) \leq i(L_1) + i(L_2).$$

PROOF. Let $\nu: X \times X \to X$ be the morphism $(x, y) \longmapsto x - y$, and set $L = p_1^*(L_1) \otimes p_2^*(L_2)$. Then $\nu^{-1}(0)$ is the diagonal of $X \times X$, and if we identify it with X, $L \mid \nu^{-1}(0)$ becomes isomorphic to $L_1 \otimes L_2$, which shows that $L|_{\nu^{-1}(x)}$ is non-degenerate for any $x \in X$ and has index $i = i(L_1 \otimes L_2)$. Hence, the direct images $R^j\nu(L)$ vanish for $j < i$, and by the Leray spectral sequence, $H^p(X \times X, L) = 0$ for $p < i$. But now,

$$H^{i(L_1)+i(L_2)}(X \times X, p_1^*(L_1) \otimes p_2^*(L_2)) = H^{i(L_1)}(X, L_1) \otimes H^{i(L_2)}(X, L_2) \neq 0,$$

so that $i(L_1) + i(L_2) \geq i = i(L_1 \otimes L_2)$.

STEP D. Let L_1 and L_2 be non-degenerate line bundles on an abelian variety X such that $L_1 \otimes L_2^{-1}$ is ample. If $f(m,n) = \chi(L_1^m \otimes L_2^n)$, suppose $f(t, 1-t)$ has a unique zero τ in $[0, 1]$ of multiplicity λ. Then

$$0 \leq i(L_2) - i(L_1) \leq \lambda.$$

PROOF. By Step C, we have

$$i(L_1) = i(L_1 \otimes L_2^{-1} \otimes L_2) \leq i(L_1 \otimes L_2^{-1}) + i(L_2) = i(L_2)$$

which proves the first inequality.

Since f is homogeneous and $i(L^n) = i(L)$ for $n > 0$, we may replace L_1 and L_2 by suitable powers to suppose $L_1 \otimes L_2^{-1}$ very ample. Let us denote by $H, H^2, \ldots$, respectively a hyperplane section of X, a hyperplane section of this section, etc. for the projective imbedding given by $L_1 \otimes L_2^{-1}$.

Let N be any large integer, which we suppose coprime to the denominator of τ if τ is rational. Then there is a unique integer r with $0 < r \leq N$ such that $\frac{r-1}{N} < \tau < \frac{r}{N}$. Put $s = N - r$, $i(L_1) = i_1$ and $i(L_2) = i_2$.

We first propose to show by induction on α that for $k < r-1$, $l = N-k$, we have

$$H^p(H^\alpha, L_1^k \otimes L_2^l) = (0) \text{ if } p < i_2 - \alpha - 1.$$

The assertion is obvious for $\alpha = 0$, since by Step B,

$$i(L_1^{r-1} \otimes L_2^{s+1}) = i(L_1^{r-2} \otimes L_2^{s+2}) = \ldots = i(L_2^N) = i_2.$$

Suppose then that $\alpha > 0$ and the above holds for $\alpha - 1$ instead of α. From the exact sequence

$$0 \longrightarrow L_1^{k-1} \otimes L_2^{l+1}|_{H^{\alpha-1}} \longrightarrow L_1^k \otimes L_2^l|_{H^{\alpha-1}} \longrightarrow L_1^k \otimes L_2^l|_{H^\alpha} \longrightarrow 0$$

we get the exactness of

$$H^p(L_1^k \otimes L_2^l|_{H^{\alpha-1}}) \longrightarrow H^p(L_1^k \otimes L_2^l|_{H^\alpha}) \longrightarrow H^{p+1}(L_1^{k-1} \otimes L_2^{l+1}|_{H^{\alpha-1}})$$

and the assertion follows by induction hypothesis. But now, the exactness of

$$H^p(L_1^{r-1} \otimes L_2^{s+1}|_{H^{\alpha-1}}) \longrightarrow H^p(L_1^r \otimes L_2^s|_{H^{\alpha-1}}) \longrightarrow H^p(L_1^r \otimes L_2^s|_{H^\alpha})$$

coupled with the above fact gives us that the map

$$H^p(L_1^r \otimes L_2^s|_{H^{\alpha-1}}) \longrightarrow H^p(L_1^r \otimes L_2^s|_{H^\alpha})$$

is injective for $p \leqslant i_2 - \alpha$. Taking $p = i_1$, we deduce that

$$H^{i_1}(X, L_1^r \otimes L_2^s) \longrightarrow H^i(H^{i_2-i_1}, L_1^r \otimes L_2^s|_{H^{i_2-i_1}})$$

is injective. Thus we deduce that

$$\dim H^{i_1}(L_1^r \otimes L_2^s|_{H^{i_2-i_1}}) \geqslant \dim H^{i_1}(L_1^r \otimes L_2^s) =$$

$$= |\chi(L_1^r \otimes L_2^s)| = N^g \left| f\left(\frac{r}{N}, \frac{s}{N}\right)\right|.$$

By the first lemma, we therefore deduce that there is a constant $c > 0$ such that for all large N (prime to the denominator of τ if τ is rational),

$$N^g \left| f\left(\frac{r}{N}, \frac{s}{N}\right)\right| < c.\, N^{g-(i_2-i_1)},$$

or

$$\left| f\left(\frac{r}{N}, \frac{s}{N}\right)\right| < \frac{c}{N^{i_2-i_1}}.$$

Now, $f(t, 1-t) = (t-\tau)^\lambda g(t)$ where g is non-vanishing at τ. Thus for all large N as above, there is a $c' > 0$ such that

$$\left|\frac{r}{N} - \tau\right|^\lambda < \frac{c'}{N^{i_2-i_1}},$$

or

$$\left|\frac{r}{N} - \tau\right| < c'' N^{-(i_2-i_1)/\lambda}.$$

If τ were rational and N coprime to the denominator q of τ, we must have $\left|\frac{r}{N} - \tau\right| > \frac{1}{Nq}$ for all r, so that we must have $\frac{i_2-i_1}{\lambda} < 1$, hence $i_2 < i_1 + \lambda$. If τ were irrational, by Kronecker's theorem on the density of fractional parts of $N\tau$ for τ irrational, for a sequence N_i of integers $\to \infty$, the distance of $N_i\tau$ from the nearest integer tends to $\frac{1}{2}$, so that we again deduce that $\frac{i_2-i_1}{\lambda} < 1$, hence $i_2 < i_1 + \lambda$.

This completes the proof of Step D.

PROOF OF THE THEOREM. We are given an ample L and a non-degenerate M. Let $P(n, m) = \chi(L^n \otimes M^m)$. We must prove that all the g zeroes of $P(t,1) = 0$ are real, and that $i(M)$ is the number of positive ones ($t = 0$ is not a zero, since M is non-degenerate). Choose a positive integer q so that the real zeroes $t_1, \ldots, t_k$ of $P(t, 1)$ are divided up as follows:

$$r_1 < \ldots < r_k, r_i \in \mathbf{Z},$$

$$q^{-1}(r_i - 1) < t_i < q^{-1} r_i.$$

Let λ_i be the multiplicity of the root t_i. Then by Steps B and D, we conclude that if $i(r) = i(L^r \otimes M^q)$, then

$$i(R) = i(r_k) < i(r_k - 1) = i(r_{k-1}) < i(r_{k-1} - 1) = \ldots$$

$(R > r_k)$

$$\ldots = i(r_2) < i(r_2 - 1) = i(r_1) < i(r_1 - 1) = i(S),$$

$(S < r_1 - 1)$

and

$$i(r_l - 1) - i(r_l) < \lambda_l.$$

But for large r, $L^r \otimes M^q$ is ample, hence $i(r) = 0$. And for large *negative* r, $(L^r \otimes M^q)^{-1}$ is ample, hence $i(r) = g$ by the last statement of the vanishing theorem. Therefore

$$g = i\begin{pmatrix}\text{very}\\ \text{negative}\\ r\end{pmatrix} - i\begin{pmatrix}\text{very}\\ \text{positive}\\ r\end{pmatrix} = \Big[\sum_{l=1}^{k} i(r_l - 1) - i(r_l)\Big] < \sum_{i=1}^{k} \lambda_l.$$

But $\Sigma\lambda_l$, the number of real zeroes of $P(t, 1) = 0$ is at most g, so equality holds everywhere, and $i(0) = i(M)$ is just the sum of the λ_l's for which the corresponding root t_l is positive.

COROLLARY. *Let V be a complex vector space of dimension g and U a lattice in it such that $X = V/U$ is an abelian variety. Let $L = L(H, \alpha)$ be a non-degenerate line bundle on X, so that H is a non-degenerate hermitian form on V. Then $i(L)$ equals the number of negative eigenvalues of H.*

PROOF. Choose a basis $u_1, u_2, \dots, u_{2g}$ of U over $\mathbf{Z}$ such that $u_1 \wedge u_2 \dots \wedge u_{2g}$ defines the orientation of V. Let $L_0 = L(H_0, \alpha_0)$ be an ample line bundle on X, so that H_0 is positive definite. We set $E = \operatorname{Im} H$ and $E_0 = \operatorname{Im} H_0$. We then have

$$\chi(L_0^n \otimes L) = \operatorname{pf}(nE_0 + E)$$

where E_0 and E are considered as skew symmetric matrices, using the above basis of U. Now, if we use any other positively oriented real basis of V, the Pfaffian gets multiplied by a positive scalar. Thus, if $e_1, \dots, e_g$ is a $\mathbf{C}$-basis of V, we can utilize the basis $e_1, ie_1, e_2, ie_2, \dots, e_g, ie_g$ to compute the sign of the above Pfaffian. Choose e_i such that $H_0(e_i, e_j) = \delta_{ij}$ and $H(e_i, e_j) = \lambda_i \delta_{ij}$, $\lambda_i \in \mathbf{R}^*$. Then $nE_0 + E$ has the matrix

$$\left[\begin{array}{cc|cc|c} 0 & -n-\lambda_1 & & & \\ n+\lambda_1 & 0 & & \mathbf{0} & \mathbf{0} \\ \hline & & 0 & -n-\lambda_2 & \\ & \mathbf{0} & n+\lambda_2 & 0 & \mathbf{0} \\ \hline & & & & \\ \mathbf{0} & & \mathbf{0} & & \ddots \end{array}\right]$$

and the Pfaffian of this matrix is $\prod_{1}^{g}(n+\lambda_i)$, (since its square is the determinant and it takes the value $\lambda_1 \dots \lambda_g$ for $n = 0$, hence the value 1 if all $\lambda_i = +1$). Thus, the index of L is the number of negative λ_i.

This corollary can also be deduced from the results of Andreotti and Grauert [A-G].

17. Very ample line bundles. The object of this section is to prove the following theorem.

THEOREM. *For any ample line bundle L on an abelian variety X, L^n is very ample, if $n \geqslant 3$.*

PROOF. For simplicity, we shall prove L^3 is very ample. If $n > 3$, the same proof works. Since $\dim H^0(X, L) = \chi(L) > 0$, we can choose an effective divisor D such that $\mathcal{O}_X(D)$ is isomorphic to the sheaf of sections of L. Further, D can be chosen so as not to have any multiple components, for if $k.E$ occurs in D with E irreducible and $k > 1$, kE is linearly equivalent to $\sum_{i=1}^{k} T_{x_i}^*(E)$ for $\sum_{1}^{k} x_i = 0$, and for suitable choice of the x_i, the $T_{x_i}^*(E)$ are all distinct and distinct from the other components of D.

Thus we assume D without multiple components. Note that for any $x, y \in X$, $T_x^*(D) + T_y^*(D) + T_{-x-y}^*(D) \in |3D|$. We have now to establish the following statements.

(1) Given $x_0, x_1 \in X$ with $x_0 \neq x_1$, there is a $D' \in |3D|$ such that $x_0 \in \operatorname{Supp} D'$, $x_1 \notin \operatorname{Supp} D'$.

(2) Given any tangent vector t to X at x_0, there is a $D' \in |3D|$ such that $x_0 \in \operatorname{Supp} D'$ and t is not tangential to D' (i.e. if $\phi = 0$ is a local equation of D' at x_0, $\langle t, d\phi \rangle \neq 0$).

Since we are making these assertions for any ample L, it suffices to prove (1) and (2) for any ample L with $x_0 = 0$, since the general case follows by applying the result to a translate of L.

Thus, if (1) were not true (with $x_0 = 0$), we would have that for any D as above and any $x, y \in X$,

$$0 \in \text{Supp } D - x \Rightarrow x_1 \in (\text{Supp } D - x) \cup (\text{Supp } D - y) \cup (\text{Supp } D + x + y).$$

Since we may clearly choose y such that x_1 does not belong to the last two members, we deduce that $x \in \text{Supp } D$ implies $x \in \text{Supp } D - x_1$, that is, $\text{Supp } D = \text{Supp } D - x_1$. Since the divisor D has no multiple components, this means that $T_{x_1}(D) = D$. In particular, $x_1 \in K(L)$, hence x_1 has finite order. Let x_1 generate the finite group F. We then have an étale morphism $\pi\colon X \to X/F$, and $D_1 = \pi(\text{Supp } D)$ is a closed subset pure of codimension one in X/F, which we may consider as a divisor with all components of multiplicity one. Since π is étale, $\pi^*(D_1)$ is again a divisor with all components of multiplicity one and has the same support as D, so that $D = \pi^*(D_1)$ and $\underline{L} \simeq \pi^*(\mathcal{O}_{X/F}(D_1))$. But note that

$$\begin{aligned}\dim H^0(X, \underline{L}) &= \chi(L) \\ &= (\text{Order } F).\chi(\mathcal{O}_{X/F}(D_1)) \\ &= (\text{Order } F).\dim H^0(X/F, \mathcal{O}_{X/F}(D_1)) \\ &> \dim H^0(X/F, \mathcal{O}_{X/F}(D_1)).\end{aligned}$$

Since the set of all divisors D_1 such that $\underline{L} \simeq \pi^*(\mathcal{O}_{X/F}(D_1))$ fall into a finite set of linear equivalence classes, this proves that all sections $s \in \Gamma(\underline{L})$ either define multiple divisors, or lie in one of a finite number of lower-dimensional subspaces $\pi^*\Gamma(\mathcal{O}_{X/F}(D_1))$. This is a contradiction, so (1) holds.

Similarly, suppose (2) is not true for a non-zero tangent vector t at 0, and let T be the invariant vector field defined by t. If (2) is false for all the divisors $T_x^*(D) + T_y^*(D) + T_{-x-y}^*(D)$, it follows immediately that for all $x \in \text{Supp } D$, the vector T_x is tangent to D at x. Since D has no multiple components, this is equivalent to the property:

(*) $\quad \forall\, U \subset X$ open, $\forall$ local equations $\phi = 0$ for D on U,

$$T(\phi) = \alpha.\phi, \text{ some } \alpha \in \mathcal{O}_X(U).$$

In terms of the $k[\epsilon]/(\epsilon^2)$-valued automorphism of X defined by T, (*) just says that the divisor D – a subscheme of X – is invariant. This implies that the $k[\epsilon]/(\epsilon^2)$-valued point of X defined by t is in the subgroup $K(L)$ of points leaving L invariant. Now in characteristic 0, all group schemes are reduced, so $K(L)$ is finite and discrete and this cannot hold unless $t = 0$. On the other hand, in characteristic p, let H be the smallest subgroup of $K(L)$ containing t; then $H \subset X^{(p)}$ and will be determined by its Lie algebra $\mathfrak{h}$ which will be the span of t and its p^{th} powers. It is easy to see that D will be invariant under translations by all points of H. [In fact, if $H = \text{Spec}(R)$, the action of H gives a homomorphism of R^* into the ring of differential operators on X, mapping elements of $\mathfrak{h}$ into the corresponding invariant derivations. Since $\mathfrak{h}$ generates R^*, and the sheaf of ideals $\mathcal{O}_X(-D)$ is stable under $\mathfrak{h}$ by (*), it is also stable under R^*, hence we get a homomorphism $R^* \to \text{Diff}(\mathcal{O}_D)$, i.e. an action of H on D.] Let $X' = X/H$, $D' = D/H$. From the results of §12, we find that $\pi\colon X \to X'$ is flat and surjective, that D' is a closed subscheme of X' and $D \simeq D' \times_{X'} X$. Therefore if $\mathscr{I}'$ is the sheaf of ideals of D',

$$\mathcal{O}_X(-D) \simeq \mathscr{I}' \otimes_{\mathcal{O}_{X'}} \mathcal{O}_X.$$

Since D is a divisor, $\mathcal{O}_X(-D)$ is a locally free sheaf, so by Part (B), Theorem 1, §12, $\mathscr{I}'$ is a locally free sheaf, i.e. D' is a divisor too. Now $D = \pi^*(D')$, so we compute, as before:

$$\begin{aligned}\dim H^0(X, \underline{L}) &= \deg \pi.\dim H^0(X/H, \mathcal{O}_{X/H}(D')) \\ &> \dim H^0(X/H, \mathcal{O}_{X/H}(D')).\end{aligned}$$

Exactly as before, this implies that all sections $s \in \Gamma(\underline{L})$ either define multiple divisors, or lie in one of a finite set of proper subspaces –a contradiction.

CHAPTER IV

Hom(X, X) AND THE l-ADIC REPRESENTATION

18. Etale coverings.

The main result is the following

THEOREM. (Serre-Lang.) *If X is an abelian variety, Y a variety and $f: Y \to X$ is an étale covering, then Y has a structure of abelian variety such that f becomes a separable isogeny.*

PROOF. Let Γ_m be the graph of the multiplication $m: X \times X \to X$ in $X \times X \times X$, and Γ' the inverse image in $Y \times Y \times Y$ of Γ_m by $f \times f \times f$. Since (1) $\Gamma' \to \Gamma_m$ is an étale covering, (2) $p_{12}: \Gamma_m \to X \times X$ is an isomorphism, (3) we have the commutative diagram

$$\begin{array}{ccc} \Gamma' & \longrightarrow & \Gamma_m \\ \downarrow{\scriptstyle p_{12}} & & \downarrow{\scriptstyle p_{12}} \\ Y \times Y & \xrightarrow[f \times f]{} & X \times X \end{array}$$

and (4) $f \times f$ is an étale covering, $p_{12}: \Gamma' \to Y \times Y$ is an étale covering too. Choose a point $y_0 \in Y$ such that $f(y_0) = 0$, and let Γ be the connected component of Γ' containing (y_0, y_0, y_0) (which belongs to Γ' since $f(y_0) = 0$ and $(0, 0, 0) \in \Gamma_m$). Then the restriction $p: \Gamma \to Y \times Y$ of p_{12} is again an étale covering, so that the degree of p equals the number of points of *any* fibre of p. We want to show that p is an isomorphism, or equivalently that there is one point of $Y \times Y$ whose inverse image in Γ is again a single point. Let $\sigma_1, \sigma_2: Y \to \Gamma$ be defined by $\sigma_1(y) = (y_0, y, y)$, $\sigma_2(y) = (y, y_0, y)$. (Since $\sigma_i(Y) \subset \Gamma'$ and $(y_0, y_0, y_0) \in \sigma_i(Y)$, it follows that $\sigma_i(Y) \subset \Gamma$.) Then the restriction of p to $\sigma_2(Y)$ is a bijection of $\sigma_2(Y)$ onto $Y \times \{y_0\}$. It therefore suffices to establish that $p^{-1}(Y \times \{y_0\}) = \sigma_2(Y)$, or equivalently that if $q: \Gamma \to Y$ is the restriction to Γ of $p_2: Y \times Y \times Y \to Y$, $q^{-1}(y_0) = \sigma_2(Y)$. Since $\sigma_2(Y)$ is an irreducible component of $q^{-1}(y_0)$, it suffices to show that $q^{-1}(y_0)$ is irreducible. Now, Γ is non-singular, being étale over $Y \times Y$ and hence $X \times X$,

and since it is also connected, it is irreducible. Further, the morphism $q\colon \Gamma \to Y$ is smooth, being the composite of the étale morphism $\Gamma \to Y \times Y$ and the projection $Y \times Y \xrightarrow{p_2} Y$. Finally $\sigma_1\colon Y \to \Gamma$ is a section for q. Now the assertion that $q^{-1}(y_0)$ is irreducible follows from the

LEMMA. *Let $f\colon X \to Y$ be a proper smooth morphism of irreducible varieties such that there is a section $\sigma\colon Y \to X$, $f \circ \sigma = 1_Y$. Then all fibres of f are irreducible.*

PROOF. We may assume $Y = \operatorname{Spec} A$ affine. Let $B = \Gamma(X, \mathcal{O}_X)$, so that B is an A-algebra which is a domain since X is irreducible and a finite A-module since f is proper. The morphism f factorises as $X \xrightarrow{g} \operatorname{Spec}(B) \xrightarrow{h} Y$ where $\operatorname{Spec}(B)$ is again an irreducible variety. But $g \circ \sigma$ is a section of h, and since $\dim(\operatorname{Spec} B) = \dim Y$, $g \circ \sigma$ is surjective, hence h is an isomorphism, and $A = B$.

Since f is smooth, its fibres are non-singular, and it suffices to show that they are connected. Let $0 \to K_0 \to K_1 \to \dots$ be a complex of free finitely generated A-modules giving the direct images of $\mathcal{O}_X$ universally, so that by the above, we have an exact sequence $0 \to A \to K_0 \to K_1$. Let y be any point of Y, $\mathfrak{M}$ its maximal ideal in A. Since completion with respect to the $\mathfrak{M}$-adic topology is an exact functor, we have an exact sequence $0 \to \hat{A} \to \hat{K}_0 \to \hat{K}_1$, so that $\hat{A} \simeq \varprojlim_n \operatorname{Ker}\left[\frac{K_0}{\mathfrak{M}^n K_0} \to \frac{K_1}{\mathfrak{M}^n K_1}\right]$. But now,

$$\operatorname{Ker}\left[\frac{K_0}{\mathfrak{M}^n K_0} \to \frac{K_1}{\mathfrak{M}^n K_1}\right] = H^0\left(f^{-1}(y), \mathcal{O}_X/\mathfrak{M}^n \mathcal{O}_X\right),$$

so the natural map $\hat{A} \xrightarrow{\sim} \varprojlim H^0(f^{-1}(y), \mathcal{O}_X/\mathfrak{M}^n \mathcal{O}_X)$ is a ring isomorphism. If $f^{-1}(y)$ were not connected, let $f^{-1}(y) = Z_1 \cup Z_2$, Z_i closed, $Z_1 \cap Z_2 = \emptyset$ and $Z_i \neq f^{-1}(y)$. We can find a unique $f_n \in H^0(f^{-1}(y), \mathcal{O}_X/\mathfrak{M}^n \mathcal{O}_X)$ which reduces to 1 on Z_1 and 0 on Z_2,

and $\{f_n\}$ defines an element $f \in \varprojlim H^0(\mathcal{O}_X/\mathfrak{M}^n \mathcal{O}_X) \simeq \hat{A}$ with $f^2 = f$, and $f \neq 0$ or 1. This is impossible since $\hat{A}$ is a local ring.

The lemma is proved.

Returning to the proof of the theorem, we have shown that $p_{12}\colon \Gamma \to Y \times Y$ is an isomorphism, so that $\nu = p_3 \circ p_{12}^{-1}\colon Y \times Y \to Y$ is a morphism. Since, as we saw, $\Gamma \supset \sigma_1(Y)$ and $\sigma_2(Y)$, it follows that $\nu(y, y_0) = y = \nu(y_0, y)$. Therefore, from the theorem proved in the Appendix to §4, Y is an abelian variety with composition law ν and zero element y_0. Since $f(y_0) = 0$, f is a homomorphism of abelian varieties.

REMARK. If X is an abelian variety and $f\colon Y \to X$ is an isogeny, then we can find an isogeny $g\colon X \to Y$ with $f \circ g = n_X$ for some $n > 0$. In fact, since $\ker f$ is a finite group scheme, it is killed by some integer $n > 0$, hence $\ker f \subseteq \ker(n_Y)$. Since $X \simeq Y/\ker f$, it follows that n_Y factorizes as $n_Y = g \circ f$ for a homomorphism $g\colon X \to Y$. But then $f \circ g = n_X$ too, since for all $x \in X$, $x = f(y)$ for some $y \in Y$, and therefore

$$f \circ g(x) = f(g(f(y))) = f(ny) = nf(y) = nx.$$

We can interpret our results in terms of the fundamental group $\pi_1(X)$. Recall, that if X is any non-singular variety, and $x_0 \in X$ is a base point, the group $\pi_1(X, x_0)$ is constructed as follows†: consider the set of all morphisms

$$\begin{array}{ccc} Y & \xrightarrow{\pi} & X \\ y_0 & \longmapsto & x_0 \end{array}$$

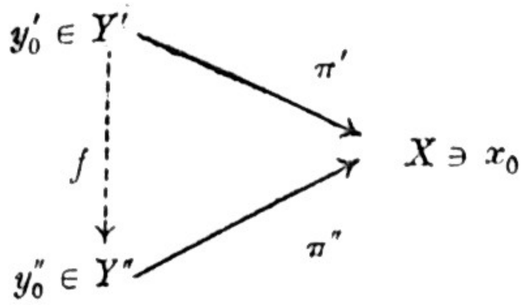
together with a base point $y_0 \in Y$ lying over x_0 such that

(1) a finite group G_Y acts freely on Y and $X \simeq Y/G_Y$ and

(2) Y is connected, hence Y is again a non-singular variety.

Given two such :

†For details, cf. [G2] pp. 60-61.



recall that there is at most one morphism $f\colon Y' \to Y''$ such that

(i) $\pi'' \circ f = \pi'$,

(ii) $f(y_0') = y_0''$.

When f exists, there is a unique surjective homomorphism

$$\rho\colon G_{Y'} \longrightarrow G_{Y''}$$

such that $f(\sigma \cdot y) = \rho(\sigma) \cdot f(y)$, all $\sigma \in G_{Y'}$, $y \in Y'$. We order the triples (Y, y_0, π) by saying $(Y', y_0', \pi') > (Y'', y_0'', \pi'')$ if such an f exists. Then the set of (Y, y_0, π)'s forms an inverse system, and we define

$$\pi_1(X, x_0) = \varprojlim_{(Y, y_0, \pi)} G_Y.$$

Now suppose X is an abelian variety and $x_0 = 0$. Then all such Y's are abelian varieties, and G_Y is just the kernel of π acting on Y by translations. In particular, we see that $\pi_1(X)$ is abelian. To describe it more explicitly, it is convenient to break it up into the product of its l-primary piece for different primes l. First suppose $l \neq p$. By the remark following the theorem, the set of étale coverings

$$X \xrightarrow{l_X^n} X$$

is cofinal in the set of all étale coverings

$$Y \xrightarrow{\pi} X, \#(\operatorname{Ker} \pi) = l^m, \text{ some } m.$$

Therefore, the l-adic component of $\pi_1(X)$ is the inverse limit of $\ker(l_X^n)$, or X_{l^n}. This is called the *l-adic Tate group* of X.

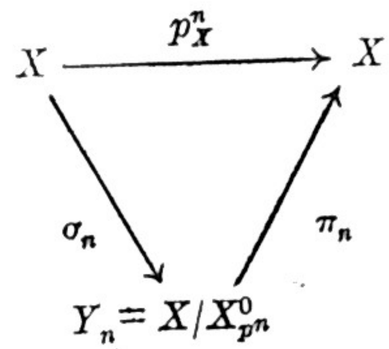
DEFINITION. $T_l(X) = \varprojlim_n X_{l^n}$, *where the inverse system is*

$$\cdots \longrightarrow X_{l^{n+1}} \xrightarrow{l_X} X_{l^n} \xrightarrow{l_X} \cdots \xrightarrow{l_X} X_l.$$

As an inverse limit of finite abelian l-torsion groups, $T_l(X)$ has the structure of a module over the l-adic integers $\mathbf{Z}_l$. Since $X_{l^n} \cong (\mathbf{Z}/l^n\mathbf{Z})^{2g}$, it is easy to see that $T_l(X) \cong \mathbf{Z}_l^{2g}$, as a $\mathbf{Z}_l$-module. Secondly suppose $l = p$. In this case, break up

$$\operatorname{Ker}(p_X^n) = X_{p^n}^0 \times X_{p^n}^r$$

where $X_{p^n}^0$ is local and $X_{p^n}^r$ is reduced. Then by the remark following the theorem, the set of étale coverings π_n in the diagrams



is cofinal in the set of all étale coverings of X whose degree is a power of p. But $\operatorname{Ker}(\pi_n) = \sigma_n(X_{p^n}^r) \cong X_{p^n}^r$, so the p-adic component of $\pi_1(X)$ is again the p-adic *discrete* Tate group.

DEFINITION. $T_p(X) = \varprojlim_n X_{p^n}^r$ (*the inverse system as before*).

$T_p(X)$ is a $\mathbf{Z}_p$-module and if $r = p$-rank of X, then clearly $T_p(X) \cong (\mathbf{Z}_p)^r$. The full fundamental group is then given by

$$\pi_1(X) \cong \prod_{\text{all primes } l} T_l(X).$$

Now suppose $k = \mathbf{C}$, and $X = V/U$ where, as usual, V is a complex vector space and U is a lattice. Then, in addition to the algebraic fundamental group as just defined, we have the usual topological fundamental group $\pi_1^{\text{top}}(X)$, which, as we saw in §1, is canonically isomorphic to U. On the other hand, since

$$X_{l^n} \cong \frac{1}{l^n} U/U \subset V/U = X,$$

it follows that

$$\begin{cases} T_l(X) \simeq \varprojlim_n \frac{1}{l^n} U/U \\ \text{with maps } \frac{1}{l^{n+1}} U/U \xrightarrow{\ l\ } \frac{1}{l^n} U/U, \end{cases}$$

i.e.

$$\begin{cases} T_l(X) \simeq \varprojlim U/l^n U \\ \text{with maps } U/l^{n+1}U \xrightarrow{\ 1\ } U/l^n U. \end{cases}$$

In other words, $T_l(X)$ is the l-adic completion of $U = \pi_1^{\text{top}}(X)$, and

$$\begin{aligned} \pi_1^{\text{alg}}(X) &= \prod_l T_l(X) \\ &= \varprojlim_n U/n!U \\ &= \text{full pro-finite completion of } U \\ &= \widehat{\pi_1^{\text{top}}}(X). \end{aligned}$$

19. Structure of $\mathrm{Hom}(X, X)$. For two abelian varieties X and Y, we denote by $\mathrm{Hom}(X, Y)$ the group of homomorphisms of X into Y, and by $\mathrm{End}\, X$ the ring $\mathrm{Hom}(X, X)$. Further we shall put $\mathrm{Hom}^0(X, Y) = \mathbf{Q} \otimes_{\mathbf{Z}} \mathrm{Hom}(X, Y)$ and $\mathrm{End}^0(X) = \mathbf{Q} \otimes_{\mathbf{Z}} \mathrm{End}\, X$ ($\mathrm{End}^0 X$ is classically called the algebra of complex multiplications of X).

Composition of homomorphisms extends to a unique $\mathbf{Q}$-bilinear map $\mathrm{Hom}^0(X, Y) \times \mathrm{Hom}^0(Y, Z) \to \mathrm{Hom}^0(X, Z)$, so that we can form a category whose objects are abelian varieties, and morphisms from X to Y are elements of $\mathrm{Hom}^0(X, Y)$, the so-called category of "abelian varieties up to isogeny". We have seen that given any isogeny $f: Y \to X$, there is another isogeny $g: X \to Y$ such that $f \circ g = n_X$, and this proves that in the new category, isogenies are isomorphisms. Thus in future, whenever we have an isogeny $f: Y \to X$, we shall denote by f^{-1} its inverse in

$\mathrm{Hom}^0(X, Y)$. It is also clear that we can give the following more fancy definition of $\mathrm{Hom}^0(X, Y)$:

$$\mathrm{Hom}^0(X, Y) = \varinjlim_{(\substack{\text{Isogenies} \\ X' \to X})} \mathrm{Hom}(X', Y).$$

THEOREM 1. (Poincaré's complete reducibility theorem.) *If X is an abelian variety and Y an abelian subvariety there is an abelian subvariety Z such that $Y \cap Z$ is finite and $Y + Z = X$. In other words, X is isogenous to $Y \times Z$.*

PROOF. Let $i: Y \to X$ be the inclusion, and $\hat{i}: \hat{X} \to \hat{Y}$ its dual homomorphism. Let L be ample on X, so that $\phi_L: X \to \hat{X}$ is an isogeny. We take Z to be the connected component of 0 of $\phi_L^{-1}(\ker \hat{i})$. We then have $\dim Z = \dim \ker \hat{i} \geqslant \dim \hat{X} - \dim \hat{Y} = \dim X - \dim Y$. Further, by definition of i and ϕ_L, if $z \in Y$, then

$$\begin{aligned} z \in \phi_L^{-1}(\ker \hat{i}) \cap Y &\iff T_z^* L \otimes L^{-1}|_Y \text{ is trivial} \\ &\iff z \in K(L|_Y). \end{aligned}$$

Since $L|_Y$ is ample, $K(L|_Y)$ and hence $Z \cap Y$ is finite. This means that the natural homomorphism $Z \times Y \to X$ has finite kernel, and since $\dim(Z \times Y) = \dim Z + \dim Y \geqslant \dim X$, it is also surjective.

REMARK. Over the complex field, the complete reducibility theorem is very simple to prove. In fact, let $X = V/U$ with V a complex vector space and U a lattice, and H a positive finite hermitian form on V which is non-degenerate with $E = \mathrm{Im}\, H$ integral on $U \times U$. Then any abelian subvariety Y of X is of the form $V_1/U \cap V_1$ where V_1 is a complex subspace of V with $V_1 \cap U$ a lattice in V_1. If V_2 is the orthogonal complement of V for H, then (a) V_2 is also the orthogonal complement of V for E, hence the lattice $U \cap V_2$ is of maximal rank in V_2; and (b) $V_1 \cap V_2 = (0)$ since H is positive definite. Thus, if $Z = V_2/V_2 \cap U$, Z is a complex subtorus of X such that $Y \cap Z$ is finite. The restriction of H to V_2 gives a Riemann form on V_2, which shows that Z is an abelian subvariety.

In fancy language, the theorem shows that the category of abelian varieties up to isogeny is a "semi-simple abelian category, all of whose objects have finite length". More concretely, we get the following corollaries by standard arguments.

DEFINITION. *An abelian variety is simple if it does not contain an abelian subvariety distinct from itself and zero.*

COROLLARY 1. *Any abelian variety X is isogenous to a product $X_1^{n_1} \times \ldots \times X_k^{n_k}$ where the X_i are simple and not isogenous to each other. The isogeny type of the X_i and the integers n_i are uniquely determined.*

(Proof standard.)

COROLLARY 2. *For X simple, the ring $\mathrm{End}^0 X$ is a division ring. For any abelian variety X, if $X = X_1^{n_1} \times \ldots \times X_k^{n_k}$, with X_i simple and not isogenous, and $D_i = \mathrm{End}^0 X_i$, then*

$$\mathrm{End}^0(X) = M_{n_1}(D_1) \oplus \ldots \oplus M_{n_k}(D_k).$$

[Here $M_k(R)$ = ring of $k \times k$ matrices over R.]

PROOF. For X simple, any non-zero endomorphism of X is an isogeny, hence an invertible element in $\mathrm{End}^0 X$, which proves the first assertion. As for the second, $\mathrm{Hom}(X_i^{n_i}, X_j^{n_j}) = (0)$ for $i \neq j$, so $\mathrm{End}^0 X = \bigoplus_{i=1}^{k} \mathrm{End}^0(X_i^{n_i})$. And $\mathrm{End}^0(X_i^{n_i})$ is clearly the algebra of matrices of order n_i on the division algebra D_i.

We shall say that a function ϕ defined on a vector space V is a polynomial function of degree n if restricted to any finite-dimensional subspace, it is a polynomial function of degree n or, equivalently, if for any $v_0, v_1 \in V$, $\phi(x_0 v_0 + x_1 v_1)$ is a polynomial in x_0 and x_1 of degree n. Thus for instance, we have seen that $\chi(L)$ extends to a homogeneous polynomial function of degree g on the vector space $NS(X) \otimes_{\mathbf{Z}} \mathbf{Q}$.

THEOREM 2. *The function $\phi \longmapsto \deg \phi$ on $\mathrm{End}\, X$ extends to a homogeneous polynomial function of degree $2g$ on $\mathrm{End}^0 X$.*

PROOF. Since for $\phi \in \mathrm{End}\, X$ and $n \in \mathbf{Z}$,

$$\deg n\phi = \deg n_X \cdot \deg \phi = n^{2g} \deg \phi,$$

it suffices to show that for $\phi, \psi \in \mathrm{End}\, X$, the function $P(n) = \deg(n\phi + \psi)$ is a polynomial function. If L is an ample line bundle, we have that

$$\deg(n\phi + \psi) = \frac{\chi((n\phi + \psi)^*(L))}{\chi(L)}.$$

Therefore it suffices to show that $\chi((n\phi + \psi)^*(L))$ is polynomial in n. Putting $L_{(n)} = (n\phi + \psi)^*(L)$ and applying Corollary 2 of the theorem of the cube to the three morphisms $n\phi + \psi$, ϕ, ϕ respectively we get that

$$L_{(n+2)} \otimes L_{(n+1)}^{-2} \otimes L_{(n)} \otimes (2\phi)^* L^{-1} \otimes \phi^* L \otimes \phi^* L = 1,$$

from which it follows by induction on n that for suitable line bundles L_1, L_2, and L_3 on X,

$$L_{(n)} = L_1^{n(n-1)/2} \otimes L_2^n \otimes L_3.$$

Since $\chi(L)$ is a polynomial function of L, $\chi(L_{(n)})$ is a polynomial in n.

To go further and prove, in particular, that $\dim_{\mathbf{Q}} \mathrm{Hom}^0(X, Y)$ is finite, it seems to be essential to use some entirely new method. If $k = \mathbf{C}$, we can compute $\mathrm{Hom}(X, Y)$ very quickly like this.

Let $X_1 = V_1/U_1$, $g_1 = \dim X_1$,

$X_2 = V_2/U_2$, $g_2 = \dim X_2$,

V_i complex vector spaces, U_i lattices.

Then every algebraic homomorphism $f : X_1 \to X_2$ lifts to a complex-analytic homomorphism $\tilde{f} : V_1 \to V_2$. As is well known, such $\tilde{f}$'s are simply the complex *linear* maps from V_1 to V_2. Conversely a complex linear map $L : V_1 \to V_2$ induces an analytic homomorphism $f : X_1 \to X_2$ if and only if $L(U_1) \subset U_2$, and by Chow's theorem (cf. §1) all analytic homomorphisms from X_1 to X_2 are algebraic.

This proves:

$$\mathrm{Hom}_{\substack{\text{abelian}\\ \text{varieties}}}(X_1,X_2) \simeq \left\{ L: V_1 \to V_2 \;\middle|\; L \text{ complex-linear},\ L(U_1) \subset U_2 \right\}.$$

In particular, L is determined by its restriction to U_1 so we get an injection

$$T\colon \mathrm{Hom}_{\substack{\text{abelian}\\ \text{varieties}}}(X_1, X_2) \longrightarrow \mathrm{Hom}_{\mathbf{Z}}(U_1, U_2).$$

Since U_i is the topological fundamental group $\pi_1^{\mathrm{top}}(X_i)$ (or the homology group $H_1(X_i)$), the map T is just the functorial representation of maps between spaces via maps between π_1's (or H_1's). If we introduce bases, we have a faithful representation of $\mathrm{Hom}(X_1, X_2)$ by $2g_1 \times 2g_2$-integral matrices. In particular, $\mathrm{Hom}(X_1, X_2)$ is a free abelian group on at most $4g_1g_2$ generators.

Even when the group field k is not $\mathbf{C}$, an analog of the above method works. This consists in using the free $\mathbf{Z}_l$-module $T_l(X)$ instead of the free $\mathbf{Z}$-module $U = \pi_1^{\mathrm{top}}(X)$. In fact $T_l(X)$ is just the l-primary component of the algebraic fundamental group $\pi_1(X)$, and when $k = \mathbf{C}$, $T_l(X)$ is nothing but the l-adic completion of U. If X_1 and X_2 are two abelian varieties, every homomorphism $f: X_1 \to X_2$ restricts to maps $f\colon (X_1)_{l^n} \to (X_2)_{l^n}$, and hence it induces a map

$$T_l(f)\colon T_l(X_1) \longrightarrow T_l(X_2).$$

The map $f \longmapsto T_l(f)$ itself is a canonical homomorphism:

$$T_l\colon \mathrm{Hom}_{\substack{\text{abelian}\\ \text{varieties}}}(X_1, X_2) \to \mathrm{Hom}_{\mathbf{Z}_l}(T_l(X_1), T_l(X_2)),$$

known as the *l-adic representation*. In fact, in terms of bases of $T_l(X_i)$ over $\mathbf{Z}_l$, this represents homomorphisms f by $2g_1 \times 2g_2$ matrices with coefficients in $\mathbf{Z}_l$. We now prove

THEOREM 3. *For any pair of abelian varieties X and Y, $\mathrm{Hom}(X, Y)$ is a finitely generated free abelian group, and the natural map*

$$\mathbf{Z}_l \otimes_{\mathbf{Z}} \mathrm{Hom}(X, Y) \longrightarrow \mathrm{Hom}_{\mathbf{Z}_l}(T_l(X), T_l(Y)) \qquad (*)$$

induced by T_l: $\mathrm{Hom}(X, Y) \to \mathrm{Hom}_{\mathbf{Z}_l}(T_l(X), T_l(Y))$ (l any prime $\neq$ char k) is injective.

PROOF. Note that since $\mathrm{Hom}(X, Y)$ is torsion free, we have an inclusion $\mathrm{Hom}(X, Y) \subset \mathrm{Hom}^0(X, Y)$.

Step I. For any finitely generated subgroup M of $\mathrm{Hom}(X, Y)$,

$$\mathbf{Q}M \cap \mathrm{Hom}(X, Y) = \{\phi \in \mathrm{Hom}(X, Y) \mid n\phi \in M, \text{ some } n \neq 0\}$$

is again finitely generated.

To prove this, choose isogenies $\prod X_i^{n_i} \to X$ and $Y \to \prod Y_j^{m_j}$ where X_i, Y_j are simple abelian varieties. Then $\mathrm{Hom}(X, Y)$ gets mapped injectively into $\prod_{i,j} \mathrm{Hom}(X_i, Y_j)$, so that it suffices to prove this result for X and Y simple. If X and Y are not isogenous, $\mathrm{Hom}(X, Y) = (0)$, so that we may assume that they are; in this case using the injection $\mathrm{Hom}(X, Y) \to \mathrm{End}\ X$ induced by an isogeny $Y \to X$, we are reduced to the case $X = Y$ and X simple. By the earlier theorem, there is a homogeneous polynomial function P on $\mathrm{End}^0 X$ such that for $\phi \in \mathrm{End}\, X$, $P(\phi) = \deg \phi \in \mathbf{Z}$. Since any $\phi \neq 0$ is an isogeny, $P(\phi) \geqslant 1$ if $\phi \in \mathrm{End}\, X$ and $\phi \neq 0$. Now $\mathbf{Q}.M$ is a finite-dimensional space, and $|P(\phi)| < 1$ is a neighborhood U of 0 in this space. Therefore $U \cap \mathrm{End}\,(X) = (0)$, so $\mathrm{End}\, X \cap \mathbf{Q}.M$ is discrete in $\mathbf{Q}.M$ and hence is finitely generated.

Step II. For any $l \neq p$, the map (*) is injective.

In fact, it suffices to show, in view of Step I, that for any finitely generated (hence free) submodule M of $\mathrm{Hom}(X, Y)$ such that $M = \mathbf{Q}.M \cap \mathrm{Hom}(X, Y)$,

$$\mathbf{Z}_l \otimes_{\mathbf{Z}} M \longrightarrow \mathrm{Hom}_{\mathbf{Z}_l}(T_l(X), T_l(Y))$$

is injective. Let $f_1, \ldots, f_p$ be a $\mathbf{Z}$-base of M. If this map is not injective, since the right side is $\mathbf{Z}_l$-free, we can find $\alpha_i \in \mathbf{Z}_l$ with at least one α_i a unit such that $\Sigma\, \alpha_i f_i \longmapsto 0$. Hence we can find integers n_i ($1 \leqslant i \leqslant p$) not all $\equiv 0 \pmod{l}$ such that $T_l(\sum_1^p n_i f_i)$ maps $T_l(X)$ into $lT_l(Y)$. By the very definition of $T_l(f)$, this

means that $\sum_1^p n_i f_i = f$ maps X_l into 0. But then, f factorizes as $X \xrightarrow{l} X \xrightarrow{g} Y$, and since $g \in \mathbf{Q}.M \cap \mathrm{Hom}(X, Y) = M$, $g = \sum_1^p m_i f_i$. Thus $\Sigma n_i f_i = l\Sigma m_i f_i$, and $f_1, \ldots, f_p$ being a basis of M, $l \mid n_i$ for all i, a contradiction.

The theorem now follows. In fact, because of the injectivity of (*), $\mathrm{Hom}^0(X, Y)$ is finite-dimensional over $\mathbf{Q}$, and because of Step I, $\mathrm{Hom}(X, Y)$ is finitely generated, and being torsion free, it is also free.

COROLLARY 1. $\mathrm{Hom}(X, Y) \simeq \mathbf{Z}^\rho$ *with* $\rho \leqslant 4\dim X.\dim Y$.

PROOF. In fact, the rank of $\mathrm{Hom}(X, Y)$ is at most that of $\mathrm{Hom}_{\mathbf{Z}_l}(T_l(X), T_l(Y))$ which is $4\dim X.\dim Y$.

COROLLARY 2. *For any abelian variety* X, *the group* $NS(X) = \mathrm{Pic}X/\mathrm{Pic}^0X$ *is free of finite rank* (*called the base number of* X).

PROOF. In fact, the homomorphism $L \longmapsto \phi_L$ induces an injection of $NS(X)$ into $\mathrm{Hom}(X, X)$.

COROLLARY 3. End^0X *is a finite-dimensional semisimple algebra over* $\mathbf{Q}$.

Let A be a finite-dimensional associative algebra over a field Γ, which, for simplicity, we assume to be infinite. By a *trace form* on A over Γ, we mean a Γ-linear form

$$S: A \longrightarrow \Gamma$$

such that $S(XY) = S(YX)$ for $X, Y \in A$. A *norm form* on A over Γ is a non-zero polynomial function

$$N: A \longrightarrow \Gamma$$

(i.e. in terms of a basis of A over Γ, $N(a)$ can be written as a polynomial over Γ in the components of a) such that $N(XY) = N(X).N(Y)$ for $X, Y \in A$. The following lemma is well known, but we include a proof for the sake of completeness.

LEMMA. *Let* A *be a finite-dimensional associative simple algebra over a field* Γ (*assumed infinite*) *with center* Λ, *separable over* Γ. *There is a canonical norm form* N^0 *and a canonical trace form* Tr^0 *of* A *over* Λ *such that any norm form* (*resp. trace form*) *of* A *over* Γ_0 *is of the type* $(\mathrm{Nm}_{\Lambda/\Gamma} \circ N^0)^k$ *with* k *an integer* $\geqslant 0$ (*resp.* $\phi \circ \mathrm{Tr}^0$ *where* $\phi: \Lambda \to \Gamma$ *is a* Γ-*linear form*). *If* $[A:\Lambda] = d^2$, N^0 *is homogeneous of degree* d.

PROOF. When $\Gamma = \Lambda$ is separably closed, A can be taken to be a matrix algebra $M_d(\Gamma)$. In this case, the elements $XY - YX$ span the vector subspace of matrices of zero trace, and any norm form gives rise to a rational homomorphism of algebraic groups $GL(d) \to \mathbf{G}_m$. This shows the validity of the lemma with Tr = matrix trace, N = matrix determinant.

In the general case, let $\overline{\Gamma}$ be the separable closure of Γ, $\sigma_i: \Lambda \to \overline{\Gamma}$ $(1 \leqslant i \leqslant [\Lambda:\Gamma])$ the various imbeddings of Λ in $\overline{\Gamma}$ over Γ, and $\overline{\Gamma}_{(i)}$ the field $\overline{\Gamma}$ considered as a Λ-algebra through σ_i. We have an isomorphism of $\overline{\Gamma}$-algebras

$$A \otimes_\Gamma \overline{\Gamma} \simeq A \otimes_\Lambda (\Lambda \otimes_\Gamma \Gamma) \simeq \prod_i A \otimes_\Lambda \overline{\Gamma}_{(i)}.$$

Denote the image of $\alpha \in A \otimes_\Gamma \overline{\Gamma}$ under this isomorphism by $\{\phi_i(\alpha)\}$. If N is any norm form on A over Γ, it extends to a norm form of $A \otimes_\Gamma \overline{\Gamma}$ over $\overline{\Gamma}$, and defines a norm form N_i on $A \otimes_\Gamma \overline{\Gamma}_{(i)}$ by the equation $N_i(\xi) = N(1, 1, \ldots, \xi, 1, \ldots, 1)$. By what we have seen, $N_i = (N_i^0)^{n_i}$, where N_i^0 is the reduced norm of $A \otimes_\Lambda \overline{\Gamma}_{(i)}$ over $\overline{\Gamma}_{(i)}$ so that we get

$$N(\alpha) = \prod_i N_i^0(\phi_i(\alpha))^{n_i}.$$

We shall show that the norm $\alpha \longmapsto \prod_i N_i^0(\phi_i(\alpha))^{n_i}$ of $A \otimes_\Gamma \overline{\Gamma}$ over $\overline{\Gamma}$ comes from a norm of A over Γ by base extension if and only if all the n_i are equal. Since $\overline{\Gamma}$ is the separable closure of Γ, N comes from Γ if and only if for any automorphism σ of $\overline{\Gamma}$ over Γ, we have $N((1 \otimes \sigma)\alpha) = \sigma(N\alpha)$, that is to say,

$$\prod_i N_i^0(\phi_i((1\otimes\sigma)\alpha))^{n_i} = \sigma\prod_i N_i^0(\phi_i(\alpha))^{n_i}.$$

Now, there is a permutation π of the integers from 1 to $[\Lambda:\Gamma]$ such that $\sigma\circ\sigma_i = \sigma_{\pi(i)}$, and we have the commutative diagram

$$\begin{array}{ccc} A\otimes_\Gamma\bar{\Gamma} & \xrightarrow{\phi_i} & A\otimes_\Lambda\bar{\Gamma}_{(i)} \\ \downarrow{\scriptstyle 1\otimes\sigma} & & \downarrow{\scriptstyle 1\otimes\sigma} \\ A\otimes_\Gamma\bar{\Gamma} & \xrightarrow{\phi_{\pi(i)}} & A\otimes_\Lambda\bar{\Gamma}_{\pi(i)} \end{array}$$

so that (since the second vertical arrow is an isomorphism of simple algebras over the isomorphism σ of separably closed base fields) we get $N^0_{\pi(i)}[\phi_{\pi(i)}((1\otimes\sigma)(\alpha))] = \sigma N_i^0(\phi_i(\alpha))$, and on substitution, we see that we must have $n_{\pi(i)} = n_i$ for all i. Now, the Galois group of $\bar{\Gamma}$ over Γ acts transitively on the imbeddings over Λ in $\bar{\Gamma}$, so that we must have all the n_i equal.

Thus we see that we may take $N^0(\alpha) = \prod_i N_i^0(\phi_i(\alpha))$ in the lemma, and then $N(\alpha) = \mathrm{Nm}_{\Lambda/\Gamma}(N^0_{A/\Lambda}(\alpha))^{n_i}$. The assertion about the trace is even simpler.

DEFINITION. *$\mathrm{Nm}_{\Lambda/\Gamma}\circ N^0$ will be called the reduced norm of A over Γ and $\mathrm{Tr}_{\Lambda/\Gamma}\circ\mathrm{Tr}^0$ will be called the reduced trace of A over Γ.*

We can now prove the following important

THEOREM 4. *Let f be an endomorphism of an abelian variety, and $T_l(f)$ the induced endomorphism of $T_l(X)$ ($l\neq$ characteristic). Then*

$$\deg f = \det T_l(f),$$

hence

$$\deg(n.1_X - f) = P(n),$$

where $P(t)$ is the characteristic polynomial, $\det(t - T_l(f))$, of $T_l(f)$. The polynomial P is monic of degree $2g$, has rational integral coefficients, and $P(f) = 0$.

PROOF. The functions $f\longmapsto \deg f$ and $f\longmapsto \det T_l(f)$ both extend uniquely to norm forms N_1 and N_2 respectively of degree $2g$ on the semi-simple $\mathbf{Q}_l$-algebra $\mathbf{Q}_l\otimes_{\mathbf{Z}}$ End X, where $\mathbf{Q}_l$ is the quotient field of $\mathbf{Z}_l$. If $|\ \ |$ denotes the l-adic absolute value, we assert that $|N_1\alpha| = |N_2\alpha|$ for all $\alpha\in\mathbf{Q}_l\otimes_{\mathbf{Z}}$ End X. In fact, it suffices to verify this by homogeneity for $\alpha\in\mathbf{Z}_l\otimes_{\mathbf{Z}}$ End X, and by continuity for $\alpha\in$ End X. Thus we have to show that the power of l dividing $\deg f$ equals the power of l dividing $\det T_l(f)$. Now, the power of l dividing $\deg f$ is the order of the kernel of $X_{l^n}\xrightarrow{f} X_{l^n}$ for n large, or what is the same the order of the cokernel of this map for n large. On passing to the limit, it is also the order of the cokernel of $T_l(f)$, which is l^ν, where ν is the power of l occurring in $\det T_l(f)$.

Now let $\mathbf{Q}_l\otimes_{\mathbf{Z}}\mathrm{End}\ X\simeq\prod_{j=1}^r A_j$ be the decomposition of $\mathbf{Q}_l\otimes_{\mathbf{Z}}$ End X into a product of simple algebras. The norms N_1 and N_2 go over into norms on $\prod_j A_j$, i.e. into power products

$$N_i(\alpha_1,\ldots,\alpha_p) = \prod_{j=1}^r N_j^0(\alpha_j)^{\nu_{ij}}\ (i=1,2),$$

where N_j^0 are the norm forms on A_j over $\mathbf{Q}_l$ of lowest degree, by the lemma. On taking $\alpha_j = 1$ for $j\neq j_0$, we deduce that $|N_{j_0}(\alpha_{j_0})|^{\nu_{1j_0}-\nu_{2j_0}} = 1$ for all $\alpha_{j_0}\in A_{j_0}$. Since N_{j_0} is homogeneous of positive degree, we see (by multiplying α_{j_0} by l) that $\nu_{1j_0} = \nu_{2j_0}$, and since this holds for all j_0, $N_1 = N_2$.

This proves the first statement of the theorem. The second follows on substituting $n.1_X - f$ for f and using $T_l(n.1_X - f) = n.1_{T_l(X)} - T_l(f)$. Now P has to be monic of degree $2g$ and, since $P(n)$ is an integer for all n, its coefficients are all rational. Further, since End X is a finite $\mathbf{Z}$-module, f is integral over $\mathbf{Z}$, so f and hence $T_l(f)$ satisfies a monic equation over $\mathbf{Z}$. Hence all the eigenvalues of the matrix $T_l(f)$ are algebraic integers, and its characteristic polynomial has coefficients which are algebraic integers. Since the coefficients are also

rational, they are rational integers. Hence $P(f)$ is a well-defined element of $\mathrm{End}\,X$, and we have finally $T_l(P(f)) = P(T_l f) = 0$, so that $P(f) = 0$.

DEFINITION. *The above polynomial $P(t)$ (which belongs to $\mathbf{Z}[t]$ and is independent of l) is called the characteristic polynomial of f. Its constant term and minus the coefficient of t^{g-1} are called the norm and trace respectively of f.*

By the lemma proved earlier, we see that if $\mathrm{End}^0X = A_1 \times \ldots \times A_k$ where A_i are simple algebras over $\mathbf{Q}$, and we denote the components of an $f \in \mathrm{End}^0X$ in A_i by f_i, and the reduced norm of A_i over $\mathbf{Q}$ and the reduced trace over $\mathbf{Q}$ by Nm^0 and Tr^0 respectively, we have

$$\mathrm{Nm}\, f = \prod_{i=1}^{k} (\mathrm{Nm}^0 f_i)^{n_i},$$

$$\mathrm{Tr}\, f = \sum_{i=1}^{k} n_i \mathrm{Tr}^0 f_i,$$

where n_i are integers > 0.

COROLLARY. *Let X be a simple abelian variety of dimension g, K the center of the algebra* End^0X, $[K:\mathbf{Q}] = e$, $[\mathrm{End}^0X : K] = d^2$. *Then de divides $2g$.*

PROOF. We have $\mathrm{Nm}\, f = (\mathrm{Nm}^0 f)^n$ for some n. But Nm is a polynomial function of degree $2g$, and Nm^0 is a polynomial function of degree de.

REMARK. When the characteristic of k is zero, with assumptions as in the above corollary, one can say even that d^2e divides $2g$. In fact, we may assume (by the Lefschetz principle) that k is the complex field. Let $X = V/U$ as usual. Then the division ring End^0X admits a faithful representation in the rational vector space $U \otimes \mathbf{Q}$, so $U \otimes \mathbf{Q}$ becomes a vector space over End^0X. Hence $\dim_{\mathbf{Q}} U \otimes \mathbf{Q} = 2g$ must be divisible by $\dim_{\mathbf{Q}} \mathrm{End}^0X = d^2e$.

This is definitely false in positive characteristic. In fact, for any characteristic $p > 0$, we shall see in §22 that there exists an

elliptic curve X with p-rank 0 and that for such a curve, End^0X is non-commutative of rank 4 with center $\mathbf{Q}$. Thus, in this case, $de = 2 = 2g$.

DEFINITION. *A simple abelian variety X is of (CM)-type if $de = 2g$ where d^2 is the rank of* End^0X *over its center K, e is the degree of K over $\mathbf{Q}$ and g the dimension of X.*

Now, in a division algebra A of rank d^2 over its center K it is well known that all maximal commutative subfields have degree d over K. Thus, a simple abelian variety X is of (CM)-type if and only if End^0X admits a subfield of degree $2g$ (since in any case, $de \leq 2g$).

20. Riemann forms. Let l be a prime different from the characteristic of k, and let μ_{l^n} be the group of l^n-th roots of unity in k^*. We have homomorphisms $\mu_{l^{n+1}} \to \mu_{l^n}$ given by $\xi \longmapsto \xi^l$, and this makes $\{\mu_{l^n}\}$ a projective system. Let us put $M_l = \varprojlim \mu_{l^n}$.

M_l has the structure of $\mathbf{Z}_l$-module. Since evidently we can choose isomorphisms $\mu_{l^n} \simeq \mathbf{Z}/l^n\mathbf{Z}$ such that the maps $\mu_{l^{n+1}} \to \mu_{l^n}$ go over into the natural maps $\mathbf{Z}/l^{n+1}\mathbf{Z} \to \mathbf{Z}/l^n\mathbf{Z}$ the projective limit is (non canonically) isomorphic to the $\mathbf{Z}_l$ itself.

Now, let n be any integer prime to the characteristic. We have set up a canonical isomorphism of $\ker n_{\hat{X}}$ with the dual of $\ker n_X$, that is to say, we have defined a pairing which we will call $\bar{e}_n$: $X_n \times (\hat{X})_n \to \mu_n$, where μ_n is the group of n-th roots of unity in k^*. Recall the definition:

Take $a \in X_n$ and $\lambda \in (\hat{X})_n$, and let λ correspond to the line bundle L. Then L^n is trivial, so $n_X^* L$ is trivial too and

$$L \simeq \mathbf{A}^1 \times X \Big/ \left\{ \begin{array}{l} \text{action of } X_n \\ \\ \phi_u(\alpha, x) = (\chi(u).\alpha,\ x + u) \end{array} \right\}$$

for a character $\chi\colon X_n \to k^*$. Then

$$\bar{e}_n(a, \lambda) = \chi(a).$$

In other words, we take the canonical action of X_n on $n_X^* L$ and carry it over to an action of X_n on the trivial bundle, where it is given by a character χ. It is useful to have an alternate definition of $\bar{e}_n$ using divisors instead of line bundles. Let D be a divisor such that

$$\mathcal{O}_X(D) \simeq \underline{L}.$$

Since L^n and $n_X^* L$ are trivial, there are rational functions f and g on X such that

$$(f) = nD,$$

$$(g) = n_X^{-1}(D).$$

Then

$$(n_X^* f) = n.n_X^{-1} D = (g^n),$$

so for some constant α,

$$g^n(x) = \alpha . f(n . x), \text{ all } x \in X.$$

It follows that $[g(x)/g(x+a)]^n = 1$ for all $x \in X$, i.e. $g(x)/g(x+a)$ is a constant n-th root of unity, and we can prove

LEMMA. $\bar{e}_n(a,\lambda) = \dfrac{g(x)}{g(x+a)}$.

PROOF. Let $\dfrac{g(x)}{g(x+a)} = \eta(a)$. Consider the diagram of maps of sheaves:

$$\mathcal{O}_X(D) \xrightarrow{n_X^*} \mathcal{O}_X(n_X^{-1}D) \xleftarrow[\text{mult. by } g]{\approx} \mathcal{O}_X.$$

It follows that for all affine open sets $U \subset X$, if $V = n_X^{-1}(U)$, then we get a diagram

$$\Gamma(U,\mathcal{O}_X(D)) \xrightarrow{n_X^*} \Gamma(V, \mathcal{O}_X(n_X^{-1}D)) \xleftarrow[\text{mult. by } g]{\approx} \Gamma(V,\mathcal{O}_X)$$

and this identifies $\Gamma(U,\mathcal{O}_X(D))$ with the subspace of $\Gamma(V,\mathcal{O}_X)$ of functions $f(x)$ such that

$$f(x+u) . g(x+u) = f(x) . g(x), \text{ all } u \in X_n.$$

On the other hand, if we let M be the quotient of $\mathbf{A}^1 \times X$ by the action of X_n

$$\phi_u(\alpha, x) = (\eta(u).\alpha, x+u),$$

then $\Gamma(U, \underline{M})$ is identified with the subspace of $\Gamma(V,\mathcal{O}_X)$ of functions $f(x)$ such that

$$\phi_u(f(x), x) = (f(x+u), x+u), \quad \text{all } u \in X_n,$$

i.e. $f(x+u) = \eta(u) . f(x)$, all $u \in X_n$. This is the same condition as before, so $\underline{M} \simeq \mathcal{O}_X(D)$, i.e., $M \simeq L$. Therefore η must equal χ.

We want to pass to the limit over n, by means of the

PROPOSITION. *Let m, n be two integers coprime to the characteristic, $x \in X_{mn}$, $y \in (\hat{X})_{mn}$. We then have*

$$\bar{e}_n(mx, my) = (\bar{e}_{mn}(x, y))^m.$$

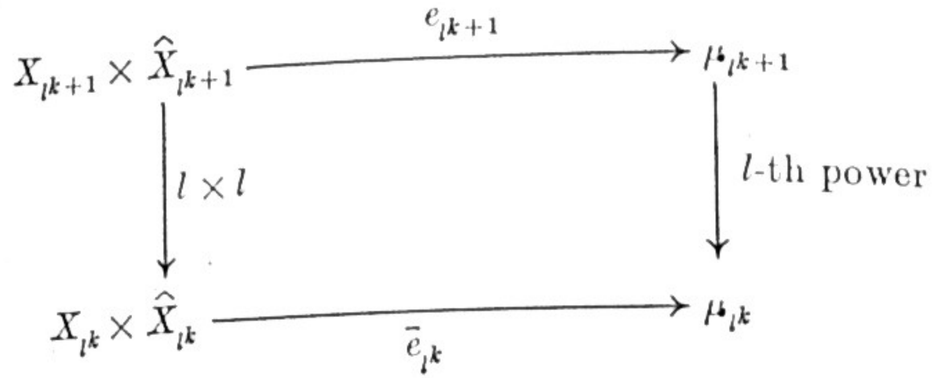
PROOF. Let V be a complete variety, G a finite group acting freely on V, H a normal subgroup of G, L a line bundle on V/G which becomes trivial when pulled back to V/H. Then we get an associated homomorphism χ of G/H into k^* as above. But now, L becomes trivial also when pulled back to V, and we thus get a homomorphism χ' of G into k^*. It is then clear that $\chi' = \chi \circ \eta$ where $\eta: G \to G/H$ is the natural homomorphism.

Let us now apply this remark with $V = X$, $G = X_{mn}$ and $H = X_m$. The quotients $X \to X/G$, $X \to X/H$ and $X/H \to X/G$ identify themselves to the maps $(mn)_X: X \to X$, $m_X: X \to X$ and $n_X: X \to X$ respectively, and the natural homomorphism $G \to G/H$ becomes $X_{mn} \xrightarrow{m_X} X_n$. Hence, for any line bundle L on X such that $n_X^*(L)$ is trivial, and any $x \in X_{mn}$, we have by the above that

$$\bar{e}_n(mx, \lambda) = \bar{e}_{mn}(x, \lambda),$$

where $\lambda \in \hat{X}_n$ corresponds to L. Writing $\lambda = my$ with $y \in (\hat{X})_{mn}$, the proposition follows.

In particular, taking $n = l^k$ and $m = l$, we get the commutative diagram



and hence by passage to the limit as $k \to \infty$, we get a natural pairing

$$e_l\colon T_l(X) \times T_l(\hat{X}) \longrightarrow M_l.$$

One checks trivially that this pairing is $\mathbf{Z}_l$-bilinear and non-degenerate. Further, if $f\colon X \to Y$ is a homomorphism of abelian varieties, $\hat{f}$ its dual and $T_l(f)$ and $T_l(\hat{f})$ are the homomorphisms induced on the Tate modules, we have for $\xi \in T_l(X)$ and $\eta \in T_l(\hat{Y})$,

$$e_l(T_l(f)\,(\xi), \eta) = e_l(\xi, T_l(\hat{f})\,(\eta)). \tag{I}$$

This follows from a corresponding equation for $\bar{e}_n$, which follows readily after writing out the definitions.

THE RIEMANN FORM OF A DIVISOR.

DEFINITION. *Let L be a line bundle on an abelian variety X, and l a prime distinct from the characteristic of k. We then define the Riemann form E^L of L to be the $\mathbf{Z}_l$-bilinear map $E^L\colon T_l(X) \times T_l(X) \to M_l$ given by $E^L(x, y) = e_l(x, T_l(\phi_L)(y))$.*

THEOREM 1. *The Riemann form E^L of any line bundle L is skew-symmetric.*

We will give a sheaf-theoretic proof of this in §23. Rather than chase through confusing diagrams, here is the proof in the language of divisors.

PROOF. It suffices to prove that $\bar{e}_n(a, \phi_L(a)) = 1$, all $a \in X_n$. Let the divisor D represent L. If $a \in X_n$, and g satisfies

$$(g) = n_X^{-1}(T_a^{-1}D - D),$$

then we must prove that $g(x + a) = g(x)$, all $x \in X$. Choose b such that $nb = a$, and let $E = n_X^{-1}D$, so

$$(g) = T_b^{-1}E - E.$$

Then

$$(T_{ib}^{*}g) = T_{(i+1)b}^{-1}E - T_{ib}^{-1}E,$$

and since E is invariant under T_a,

$$\left(\prod_{i=0}^{n-1} T_{ib}^{*}g\right) = \sum_{i=0}^{n-1} T_{(i+1)b}^{-1}E - T_{ib}^{-1}E = 0.$$

Therefore $h(x) = \prod_{i=0}^{n-1} g(x + ib)$ is a constant, hence

$$1 = \frac{h(x+b)}{h(x)} = \frac{\prod_{i=0}^{n-1} g(x + b + ib)}{\prod_{i=0}^{n-1} g(x + ib)} = \frac{g(x+a)}{g(x)}.$$

Thus $L \longmapsto E^L$ induces a map:

$$\begin{array}{c} NS(X) \\ \| \text{def} \\ \mathrm{Pic}(X)/\mathrm{Pic}^0(X) \end{array} \longrightarrow \left\{ \begin{array}{l} \text{Alternating 2-forms} \\ T_l(X) \times T_l(X) \to M_l \end{array} \right\}.$$

This is injective since $E^L = 0 \Rightarrow \phi_L = 0$ since e_l is non-degenerate. Now, if $f\colon X \to Y$ is a homomorphism of abelian varieties, and L is a line bundle on Y, then

$$E^{f^*L}(x, y) = E^L(T_l f(x), T_l f(y)),\ x, y \in T_l X. \tag{II}$$

PROOF.
$$\begin{aligned} E^{f^*L}(x, y) &= e_l(x, \phi_{f^*L}\, y) \\ &= e_l(x, T_l\hat{f} \circ \phi_L \circ T_l f(y)) \\ &= e_l(T_l f(x), \phi_L(T_l f(y))) \\ &= E^L(T_l f(x), T_l f(y)). \end{aligned}$$

Next, we can compute E^P, when P is the Poincaré bundle on $X \times \hat{X}$. Identifying $T_l(X \times \hat{X})$ with $T_l(X) \times T_l(\hat{X})$, then

$$E^P((x, \hat{x}), (y, \hat{y})) = e_l(x, \hat{y}) - e_l(y, \hat{x}). \tag{III}$$

PROOF. By skew-symmetry and linearity, it suffices to show that $E^P((x,0),(y,0)) = E^P((0,\hat{x}),(0,\hat{y})) = 0$ and $E^P((x,0),(0,\hat{y})) = e_l(x,\hat{y})$. Using the functoriality property of E for the inclusion of $X \times (0)$ in $X \times \hat{X}$ and the triviality of the restriction of P to $X \times (0)$, it follows that $E^P((x,0),(y,0)) = 0$; similarly $E^P((0,\hat{x}),(0,\hat{y})) = 0$. To prove the last assertion note that we have an isomorphism $(X \hat{\times} Y) \xrightarrow{\sim} \hat{X} \times \hat{Y}$ which is given by the map of line bundles $L \longmapsto (L|X \times (0), L|(0) \times Y)$ for $L \in \mathrm{Pic}^0(X \times Y)$. In particular, taking $Y = \hat{X}$, we have an identification of $(X \hat{\times} \hat{X})$ with $\hat{X} \times \hat{\hat{X}}$. Now, for any $(x, \hat{x}) \in X \times \hat{X}$, $\phi_P((x,\hat{x}))$ is given by the line bundle $T^*_{(x,\hat{x})} P \otimes P^{-1}$, and this is determined by the pair of bundles

$$(T^*_{(x,\hat{x})} P \otimes P^{-1}|_{X\times(0)},\ T^*_{(x,\hat{x})} P \otimes P^{-1}|_{(0)\times\hat{X}}) \cong (P|_{X\times(\hat{x})},\ P|_{(x)\times\hat{X}}).$$

Therefore $\phi_P((x,\hat{x})) = (\hat{x}, i(x))$, where $i: X \to \hat{\hat{X}}$ is the natural homomorphism. Thus, we obtain

$$E^P((x,0),\ (0,\hat{y})) = e_l((x,0),\ (\hat{y},0)) = e_l(x,\hat{y}).$$

Theorem 1 has the following partial converse.

THEOREM 2. *Let X be an abelian variety, and $\phi: X \to \hat{X}$ a homomorphism. Then the bilinear form $(x,y) \longmapsto e_l(x,\phi y)$ on $T_l(X)$ is skew-symmetric if and only if there is a line bundle L on X such that $2\phi = \phi_L$.*

PROOF. If $2\phi = \phi_L$, $2e_l(x,\phi(y)) = e_l(x,\phi_L(y))$ is skew-symmetric by Theorem 1, hence so is $e_l(x,\phi y)$. Conversely suppose this form is skew-symmetric, and let L be the pull back of the Poincaré bundle P by the homomorphism $(1,\phi): X \to X \times \hat{X}$. Then we claim that $2\phi = \phi_L$. It suffices, because of the non-degeneracy of e_l, to show that $2e_l(x,\phi y) = e_l(x,\phi_L y)$ for any $x, y \in T_l(X)$. Now, we have

$$\begin{aligned} e_l(x,\phi_L(y)) &= E^L(x,y) = E^P((1,\phi)(x),(1,\phi)(y)) \\ &= e_l(x,\phi y) - e_l(y,\phi x) = 2e_l(x,\phi y), \end{aligned}$$

by formulas (II) and (III) and the skew-symmetry of $e_l(x,\phi y)$.

REMARK. We shall see in §23 that if $2\phi = \phi_L$ for some line bundle L, we must have $\phi = \phi_{L'}$ for another line bundle L'. Thus, the above theorem would then give a necessary and sufficient condition for a homomorphism $\phi: X \to \hat{X}$ to be of the form ϕ_L.

THE ROSATI INVOLUTION.

We fix an ample line bundle L on the abelian variety X, so that $\phi_L: X \to \hat{X}$ is an isogeny.

DEFINITION. *The Rosati involution on the algebra* $\mathrm{End}^0 X$ *with respect to* L *is the involution* $\phi' = \phi_L^{-1} \circ \hat{\phi} \circ \phi_L$, $\hat{\phi} \in \mathrm{End}^0 \hat{X}$.

One has the following properties of this map.

(1) For $\phi, \psi \in \mathrm{End}^0 X$, $(a\phi)' = a\phi'$, $a \in \mathbf{Q}$

$$(\phi + \psi)' = \phi' + \psi'$$

$$(\phi\psi)' = \psi'\phi'.$$

These are clear.

(2) Extend the homomorphism of rings T_l: End $X \to \mathrm{End}_{\mathbf{Z}_l} T_l(X)$ to a homomorphism $\mathrm{End}^0 X \to \mathrm{End}_{\mathbf{Q}_l}(\mathbf{Q}^l \otimes_{\mathbf{Z}_l} T_l(X))$ and denote the extended map again by T_l. Then for any $\phi \in \mathrm{End}^0 X$, $T_l(\phi')$ is the adjoint of $T_l(\phi)$ for the non-degenerate bilinear form E^L, that is, we have

$$E^L(\phi x, y) = E^L(x, \phi' y).$$

In particular, $\phi'' = \phi$, i.e., $\phi \longmapsto \phi'$ is an involution.

PROOF. We have

$$\begin{aligned} E^L(x,\phi' y) &= e_l(x, \phi_L \circ \phi_L^{-1} \circ \hat{\phi} \circ \phi_L y) \\ &= e_l(x, \hat{\phi} \circ \phi_L y) \\ &= e_l(\phi x, \phi_L y) \\ &= E^L(\phi x, y) \end{aligned}$$

which proves the equation.

(3) Identify $\mathbf{Q}\otimes_{\mathbf{Z}} NS(X) = \mathbf{Q}\otimes_{\mathbf{Z}} \dfrac{\operatorname{Pic} X}{\operatorname{Pic}^0 X}$ with a subspace of $\operatorname{Hom}^0(X, \hat{X})$ by the map $M \longmapsto \phi_M$. Then, under the isomorphism $\operatorname{Hom}^0(X, \hat{X}) \xrightarrow{\sim} \operatorname{End}^0 X$ given by $\psi \to \phi_L^{-1}\circ\psi$, the above subspace goes over into the subspace $\{\psi \in \operatorname{End}^0 X \mid \psi' = \psi\}$ of symmetric elements of $\operatorname{End}^0 X$ for the Rosati involution.

PROOF. In fact, by the last theorem, an element $\psi \in \operatorname{End}^0 X$ belongs to this subspace if and only if for $\phi = \phi_L \circ \psi$, we have $e_l(x, \phi y) = -\, e_l(y, \phi x)$. But this means $E^L(x, \psi y) = -\, E^L(y, \psi x)$, that is, $E^L(x, \psi y) = E^L(\psi x, y) = E^L(x, \psi' y)$, for all $x, y \in T_l(X)$. The result follows since E^L is non-degenerate and $\psi \longmapsto T_l(\psi)$ is faithful.

THEOREM 3. *Let X be an abelian variety. Then there is a generator*

$$v \in \operatorname{Hom}_{\mathbf{Z}_l}(\Lambda^{2g} T_l(X), M^{\otimes g})$$

with the following property: for all divisors $D_1, \ldots, D_g$ on X, let L_i be the line bundles $L_X(D_i)$ and let $E_i = E^{L_i}$ be their Riemann forms. Then

$$E_1 \wedge \ldots \wedge E_g = (D_1 . \ldots . D_g)\cdot v.$$

PROOF. Since both the left and the right depend in a polynomial fashion on the images of the L_i in $NS(X)$, this formula results by polarization from the formula with $L_1 = \ldots = L_g$, $D_1 = \ldots = D_g$. Using the fact that $\chi(L) = (D^g)/g!$, we are reduced to proving

$$[E^L]^{\wedge g} = g!\chi(L)\cdot v.$$

Fix an isomorphism $M_l \simeq \mathbf{Z}_l$, and choose a basis for $T_l(X)$ over $\mathbf{Z}_l$. Then $\overset{2g}{\Lambda}\, T_l(X)$ becomes isomorphic to $\mathbf{Z}_l$ by using this basis, and so that $[E^L]^{\wedge g}$ becomes a scalar. Further, by using this basis, E^L becomes a matrix. We assert that

$$([E^L]^{\wedge g})^2 = (\det\ E^L).(g!)^2.$$

In fact, this equation remains invariant under change of basis for $\mathbf{Q}_l \otimes T_l(X)$, and it follows by a simple computation on choosing a basis so that E^L takes the standard form

$$\left[\begin{array}{c|c|c} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} & \mathbf{0} & \mathbf{0} \\ \hline \mathbf{0} & \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{0} & \ddots \end{array}\right]$$

Again since both sides of the equality of the theorem are polynomials in L, we are reduced to showing that $\chi(L)^2 = c.\det E^L$, where c is an l-adic unit. By the Riemann-Roch theorem this is equivalent to: $\deg \phi_L = c.\det E^L$, where c is an l-adic unit. Now, $E^L(x, y) = e_l(x, \phi_L(y))$, and since e_l is a non-degenerate pairing over $\mathbf{Z}_l$, we see that $\det E^L = \det T_l(\phi_L)$ if we define the matrix representation of $T_l(\phi_L)$ using a dual basis of $T_l(\hat{X})$.

Choose and fix an isogeny $\psi\colon \hat{X} \to X$. We then have that

$$\begin{aligned} \deg\psi \cdot \deg\phi_L &= \deg(\psi\circ\phi_L) \\ &= \det\,[T_l(\psi)\circ T_l(\phi_L)] \\ &= \det\,(T_l(\psi))\cdot\det\,(T_l(\phi_L)). \end{aligned}$$

Thus, to complete the proof of the theorem, we have only to observe that $\deg\psi/\det T_l(\psi)$ is an l-adic unit, and this follows from the fact that the largest power of l dividing $\deg\psi$ is the order of the kernel, or equivalently cokernel, of $\psi \mid X_{l^n}\colon X_{l^n} \to X_{l^n}$ for n large and this is the same as the largest power of l dividing $\det T_l(\psi)$.

COROLLARY. *Let X be a simple abelian variety of dimension g, and $K \subset \operatorname{End}^0 X$ a $\mathbf{Q}$-subalgebra such that $\phi = \phi'$ for all $\phi \in K$. Then $[K\colon \mathbf{Q}]$ divides g.*

PROOF. Since $\phi\psi = \phi'\psi' = (\psi\phi)' = \psi\phi$ for $\phi, \psi \in K$, K is a subfield of $\operatorname{End}^0 X$. Further, since K consists of symmetric elements, it is contained in the image of $\mathbf{Q}\otimes_{\mathbf{Z}} \operatorname{Pic} X/\operatorname{Pic}^0 X$ by the map $M \longmapsto \phi_L^{-1}\circ\phi_M$. Now $\chi(M)$ depends only on the endomorphism

$\phi_L^{-1} \circ \phi_M$, and it extends to a homogeneous polynomial function of degree g on the space of symmetric elements of $\mathrm{End}^0 X$. We assert that the restriction to K of the function $\frac{\chi(M)}{\chi(L)}$ is a norm function on K. Now, it is easy to check that (since it is already polynomial), if its square $\frac{\chi^2(M)}{\chi^2(L)}$ is multiplicative on K, then it is multiplicative too. But $\frac{\chi^2(M)}{\chi^2(L)} = \frac{\deg \phi_M}{\deg \phi_L} = \deg \phi_L^{-1} \circ \phi_M$, which is multiplicative in $\phi_L^{-1} \circ \phi_M$. Thus we get a norm function of degree g on K, and K being a field of degree $[K: \mathbf{Q}]$, the corollary follows.

21. Positivity of the Rosati involution.

THEOREM 1. *Let H be an ample divisor on an abelian variety, $L = L_X(H)$ the associated line bundle and $'$ the involution of* $\mathrm{End}^0 X$ *given by L. Then for any $\phi \in \mathrm{End}\ X$, we have*

$$\mathrm{Tr}(\phi\phi') = \frac{2g}{(H^g)} (H^{g-1} . \phi^*(H))$$

where $(\ ,\ )$ denotes intersection numbers. In particular, $\phi \longmapsto \mathrm{Tr}(\phi . \phi')$ is a positive definite quadratic form on $\mathrm{End}^0 X$.

PROOF. The first assertion clearly implies the second, since for any effective divisor D and an ample divisor H, $(H^{g-1}. D) > 0$. It suffices therefore to prove the first statement.

Choose and fix bases for $T_l(X)$ and M_l. Applying Theorem 3 §19, we get

$$[E^L]^{\wedge g} = c . (H^g),$$

$$[E^L]^{\wedge g-1} \wedge E^{\phi^*(L)} = c . (H^{n-1} . \phi^*(H)),$$

for some l-adic constant c. Therefore,

$$\frac{[E^L]^{\wedge g-1} \wedge E^{\phi^*(L)}}{[E^L]^{\wedge g}} = \frac{(H^{g-1} . \phi^*(H))}{(H^g)}.$$

Since we have $E^{\phi^*(L)} = E^L \circ (\phi \times \phi)$, we are reduced to proving the equation

$$\frac{[E^L]^{\wedge g-1} \wedge (E^L \circ (\phi \times \phi))}{[E^L]^{\wedge g}} = \frac{1}{2g} \mathrm{Tr}(\phi\phi'),$$

where ϕ' is the transpose of ϕ with respect to E^L. This is purely a problem on linear algebra. We may utilize a basis $e_1, e_2, \ldots, e_{2g}$ of $\mathbf{Q}_l \otimes T_l(X)$ such that $E^L(e_{2i-1}, e_{2i}) = 1$ and $E^L(e_{2i-1}, e_j) = E^L(e_{2i}, e_j) = 0$ if $j \neq 2i$ or $2i-1$. Then the left side becomes (by definition of exterior multiplication)

$$\sum_{i_1, i_2, \ldots, i_g \text{ odd}} E^L(\phi(e_{i_g}), \phi(e_{i_g+1})) \Big| \sum_{i_1, \ldots, i_g \text{ odd}} 1$$

$$= \left[\frac{(g-1)!}{g!} \cdot \sum_{i \text{ odd}} E^L(\phi(e_i), \phi(e_{i+1})) \right]$$

$$= \frac{1}{2g} \sum_{i \text{ odd}} \left[E^L(e_i, \phi\phi'(e_{i+1})) + E^L(\phi'\phi(e_i), e_{i+1}) \right]$$

$$= \frac{1}{2g} \mathrm{Tr}(\phi'\phi).$$

APPLICATION I. STRUCTURE OF $\mathrm{End}^0 X$ FOR SIMPLE X.

We have seen that for a simple abelian variety X, $D = \mathrm{End}^0 X$ is a division algebra of finite rank over $\mathbf{Q}$ with an involution $x \longmapsto x'$ such that if $x \neq 0$, $\mathrm{Tr}(xx') > 0$ where the trace is the reduced trace over $\mathbf{Q}$ (or any positive multiple of it).

We shall now give the classification, due to Albert, of all pairs $(D, ')$ where D is a division algebra of finite rank n over $\mathbf{Q}$ and $x \longmapsto x'$ is an involution such that $\mathrm{Tr}_{D/\mathbf{Q}}(xx') > 0$ for $x \in D$, $x \neq 0$. We shall consistently use the following notations. The center of D will be denoted by K, and $K_0 = \{x \in K \mid x' = x\}$ is the set of elements of K fixed by the involution. We put $[D: K] = d^2$, $[K: \mathbf{Q}] = e$ and $[K_0: \mathbf{Q}] = e_0$ (so that $n = e.d^2$ and $e = e_0$ or $e = 2e_0$ according as the involution is trivial on K or not). Without further mention, we make use of the fact that the restriction of $\mathrm{Tr}_{D/\mathbf{Q}}$ to any simple subalgebra of $\mathbf{R} \otimes_{\mathbf{Q}} D$ is a positive multiple of the reduced trace over $\mathbf{R}$ of this subalgebra.

STEP I. Now, let $\sigma_i : K_0 \to \mathbf{R} (1 \leqslant i \leqslant r_1)$ be the set of distinct real imbeddings of K_0, and $\sigma_{r_1+j} : K_0 \to \mathbf{C}\ (1 \leqslant j \leqslant r_2)$ a set of complex imbeddings such that any non-real complex imbedding of K_0 in $\mathbf{C}$ is either a certain σ_{r_1+j} or a complex conjugate of some σ_{r_1+j}. Thus, $r_1 + 2r_2 = e_0$. We then have an isomorphism of $\mathbf{R}$-algebras

$$\sigma : \mathbf{R} \otimes_{\mathbf{Q}} K_0 \xrightarrow{\sim} \mathbf{R}^{r_1} \times \mathbf{C}^{r_2},$$

$$\sigma(1 \otimes x) = (\sigma_1(x), \ldots, \sigma_{r_1}(x), \sigma_{r_1+1}(x), \ldots, \sigma_{r_1+r_2}(x)).$$

Since the involution is the identity on K_0, for $x \in K_0^*$, we must have $\mathrm{Tr}\ x^2 > 0$, and the same must hold in $\mathbf{R} \otimes_{\mathbf{Q}} K_0$ also (in fact, this quadratic form has to be positive semi-definite on $\mathbf{R} \otimes_{\mathbf{Q}} K_0$ by continuity, and its null space, being the orthogonal complement of the whole space for this quadratic form, must be a rational subspace. But then, $\mathrm{Tr}(x.x') > 0$ for $x \in K_0$, $x \neq 0$, so that it has no null space). But this implies that $r_2 = 0$, as is trivially seen, so that K_0 is totally real.

If now $K \neq K_0$, $K = K_0(\sqrt{\alpha})$ for some $\alpha \in K_0$, $\sqrt{\alpha} \notin K_0$, and $(\sqrt{\alpha})' = -\sqrt{\alpha}$. Now, $\mathbf{R} \otimes_{\mathbf{Q}} K \simeq (\mathbf{R} \otimes_{\mathbf{Q}} K_0) \otimes_{K_0} K \simeq \prod_{i=1}^{e_0} \mathbf{R}_{(i)} \otimes_{K_0} K$ where $\mathbf{R}_{(i)}$ is $\mathbf{R}$ considered as a K_0-algebra via σ_i. Now, $\mathbf{R}_{(i)} \otimes_{K_0} K$ is isomorphic as an $\mathbf{R}$-algebra to either $\mathbf{R} \times \mathbf{R}$ or to $\mathbf{C}$ according as $\sigma_i(\alpha) > 0$ or $\sigma_i(\alpha) < 0$, and the restriction of the involution interchanges the factors in the first case and is complex conjugation in the second case. Again from the positive definiteness of $\mathrm{Tr}(x.x')$ on $\mathbf{R} \otimes_{\mathbf{Q}} K$, one deduces easily that $\mathbf{R} \times \mathbf{R}$ cannot occur as a factor, i.e., K is totally imaginary, and $\sigma_i(\alpha) < 0$ for all i. We shall say that the involution is of the *first kind* if $K = K_0$, and otherwise we say it is of the *second kind*.

STEP II. If the involution is of the first kind, the involution defines an isomorphism of D and its opposite algebra over the center K, so that its class in the Brauer group $\mathrm{Br}(K)$ of K is of order 1 or 2. If this order is one, we must have $D = K$. Next assume that the order is 2. Since by a theorem of Hasse-Brauer-Noether, the rank of a central division algebra over a number field is the square of its order in the Brauer group, D must be of rank 4 over K (i.e. a

so-called quaternion division algebra over K). In this case, there is a canonical involution $x \longmapsto x^*$ of D over K given by $x^* = \mathrm{Tr}^0_{D/K} x - x$ where Tr^0 is the reduced trace. (To check this is an involution, extend D to the algebraic closure of K, so that we are reduced to the case of a 2-by-2 matrix algebra over a field, when this is trivial to check.) By the theorem of Skolem-Noether, there is an $a \in D - \{0\}$ such that $x' = ax^*a^{-1}$ and the condition that $x'' = x$ gives us that $a^* = \epsilon . a$ with $\epsilon \in K^*$. But now, $a = a^{**} = (\epsilon.a)^* = \epsilon^2 a$, so that $\epsilon = \pm 1$.

Now, if $\epsilon = 1$, $a^* = \mathrm{Tr}_{D/K} a - a = a$, so that $a \in K$ and $x' = x^*$. We have an isomorphism

$$\mathbf{R} \otimes_{\mathbf{Q}} D \simeq (\mathbf{R} \otimes_{\mathbf{Q}} K) \otimes_K D \xrightarrow{\sim} (\mathbf{R}_{(1)} \otimes_K D) \times \ldots \times (\mathbf{R}_{(e)} \otimes_K D) \qquad (*)$$

where $\mathbf{R}_{(i)}$ is, as before, $\mathbf{R}$ considered as a K-algebra through the i-th imbedding σ_i, and each $\mathbf{R}_{(i)} \otimes_K D$ is $\mathbf{R}$-isomorphic to either the matrix algebra $M_2(\mathbf{R})$ or to the standard quaternion algebra $\mathbf{K}$ over $\mathbf{R}$. If factors of the type $M_2(\mathbf{R})$ occur, we would have that for any $A \in M_2(\mathbf{R})$, $A \neq 0$, $\mathrm{Tr}((\mathrm{Tr}\, A - A).A) > 0$, that is, $(\mathrm{Tr}\, A)^2 > \mathrm{Tr}\, A^2$, and this is false for $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Hence all the factors in the above decomposition of $\mathbf{R} \otimes_{\mathbf{Q}} D$ are isomorphic to $\mathbf{K}$ and the involution restricts on each factor to the canonical involution. Since for the standard involution on $\mathbf{K}$, we have $\mathrm{Tr}(x.x^*) > 0$ if $x \neq 0$, the conditions derived (when $\epsilon = 1$) are necessary and sufficient.

Next consider the case when $\epsilon = -1$. In the decomposition (*), let a_i be the image of a in $\mathbf{R}_{(i)} \otimes_K D = D_i$, so that on this factor, the involution takes the form $x \longmapsto a_i(\mathrm{Tr}_{D_i/\mathbf{R}}\, x - x)a_i^{-1}$, and we have also $a_i^* = \mathrm{Tr}_{D_i/\mathbf{R}}\, a_i - a_i = -a_i$, so $\mathrm{Tr}_{D_i/\mathbf{R}}\, a_i = 0$. Suppose now that D_i is $\mathbf{R}$-isomorphic to $\mathbf{K}$. Since $a_i a_i^*$ is real and positive, a_i satisfies an equation $x^2 + \lambda^2 = 0$, $\lambda \in \mathbf{R}^*$, and hence by Skolem-Noether, we can choose an isomorphism of $D_{(i)}$ with $\mathbf{K}$ such that a_i goes to $\lambda i \in \mathbf{K} = \mathbf{R} + \mathbf{R}i + \mathbf{R}j + \mathbf{R}k$. But then, if $x = x_0 + x_1 i + x_2 j + x_3 k$, we have $\mathrm{Tr}\,(x.x') = 2(x_0^2 + x_1^2 - x_2^2 - x_3^2)$ which

is not positive definite. Hence, each D_i is isomorphic to $M_2(\mathbf{R})$. Further, $K[a]$ is a subfield of D stable for the involution such that $a' = -a$, which shows that $a^2 \in K$ and a^2 is negative in every real imbedding of K. Thus, each a_i satisfies a minimal equation $a_i^2 = \lambda_i \in \mathbf{R}$ in $M_2(\mathbf{R})$ with $\lambda_i < 0$. Again by Skolem-Noether (or trivial checking) we can choose an isomorphism $\mathbf{R}_{(i)} \otimes_K D \simeq M_2(\mathbf{R})$ such that a_i goes to $\mu_i \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ with $\mu_i > 0$, $\mu_i \in \mathbf{R}$. But one checks that in this case, the involution on this factor is nothing but the transpose (in the sense of matrices), and we certainly have $\mathrm{Tr}(A.{}^tA) > 0$ for $A \in M_2(\mathbf{R})$, $A \neq 0$. Thus the conditions derived are necessary and sufficient for the positive definiteness of $\mathrm{Tr}(x.x')$.

STEP III. We come now to the case of an involution of the second kind. We summarize the results of class field theory concerning the Brauer groups of an algebraic number field and p-adic fields in the following theorem.

THEOREM. (1) *The Brauer group of a p-adic field is canonically isomorphic to $\mathbf{Q}/\mathbf{Z}$. If $L \supset K$ are two p-adic fields with $[L:K] = n$, the induced map $\mathrm{Br}(K) \to \mathrm{Br}(L)$ goes over by means of the above isomorphisms into multiplication by n in $\mathbf{Q}/\mathbf{Z}$.*

The Brauer group of $\mathbf{R}$ is cyclic of order two, and we identify it with the unique cyclic subgroup of order 2 of $\mathbf{Q}/\mathbf{Z}$.

The Brauer group of $\mathbf{C}$ is trivial.

(2) *For any central simple algebra D over an algebraic number field K, and any finite or infinite place v of K, if K_v denotes the completion of K at v, let $\mathrm{Inv}_v(K)$ denote the element of $\mathbf{Q}/\mathbf{Z}$ corresponding to the class of $D \otimes_K K_v$ in $\mathrm{Br}(K_v)$. Then we have an exact sequence*

$$0 \longrightarrow \mathrm{Br}(K) \longrightarrow \prod_v \mathrm{Br}(K_v) \longrightarrow \mathbf{Q}/\mathbf{Z} \longrightarrow 0$$

where the second map is gotten by forming the sum of the elements in $\mathbf{Q}/\mathbf{Z}$.

Let us now look at the involutorial division algebras of the second kind over $\mathbf{Q}$. Let σ be the restriction of the involution to K, so that σ induces an automorphism of $\mathrm{Br}(K)$. The existence of an involution of the second kind implies that $\sigma(\mathrm{cl}(D)) = -\mathrm{cl}(D)$, or equivalently, using the above theorem, that for any place v of K,

$$\mathrm{Inv}_v(D) + \mathrm{Inv}_{\sigma v}(D) = 0. \tag{A}$$

Since we have shown that K is totally imaginary, this condition is always fulfilled for infinite v. Suppose then that (A) holds, so that D is isomorphic to the opposite algebra to the conjugate algebra $D_{(\sigma)}$. This means that we can find a map $D \to D$, $x \longmapsto x^*$ such that for $\lambda \in K$, $(\lambda x)^* = \sigma(\lambda)x^*$, $(x+y)^* = x^* + y^*$ and $(xy)^* = y^*x^*$. By Skolem-Noether, any involution inducing σ on K must be of the form $x' = ax^*a^{-1}$ for some $a \in D$, $a \neq 0$. Since $x \longmapsto x^{**}$ is a K-automorphism of D, we must have $x^{**} = \alpha x \alpha^{-1}$ for some $\alpha \in D$, and since

$$\alpha x^* \alpha^{-1} = (x^*)^{**} = (x^{**})^* = (\alpha x \alpha^{-1})^* = \alpha^{*-1} x^* \alpha^*, \; x \in D,$$

we deduce that $\alpha^*\alpha \in K$, and since $(\alpha^*\alpha)^* = \alpha^*\alpha$, $\alpha^*\alpha \in K_0$. In order that $x \longmapsto x' = ax^*a^{-1}$ be an involution, we must have that $aa^{*-1}\alpha x \alpha^{-1} a^* a^{-1} = x$ for all $x \in D$, i.e., $a.a^{*-1}\alpha \in K$, or equivalently, $\alpha^{-1}a^* = \mu a$ for some $\mu \in K$. If we put $\phi(x) = \alpha^{-1}x^*$ for $x \in D$, then ϕ is σ-linear, and the solvability of $\phi(a) = \mu a$ with $a \neq 0$ implies that

$$(\alpha^*\alpha)^{-1} a = a(\alpha^*\alpha)^{-1} = \alpha^{-1}\alpha a \alpha^{-1}\alpha^{*-1} = \alpha^{-1}(\alpha^{-1}a^*)^* = \phi^2(a)$$
$$= \mu.\sigma\mu.a = \mathrm{Nm}_{K/K_0}\mu.a,$$

so that $\alpha^*\alpha \in \mathrm{Nm}_{K/K_0}K^*$. Conversely, if this holds, let $(\alpha^*\alpha)^{-1} = \mathrm{Nm}_{K/K_0}\lambda$, so that for any $x \in D$, if $a = \lambda x + \phi(x)$, we have

$$\phi(a) = \sigma(\lambda)\,\phi(x) + (\alpha^*\alpha)^{-1} x = \sigma(\lambda)\,(\lambda x + \phi(x)) = \sigma(\lambda).a.$$

Thus, under assumption (A), with * and α defined as above, the necessary and sufficient condition for the existence of an involution is that $\alpha^*\alpha \in \mathrm{Nm}_{K/K_0}K^*$. Since K/K_0 is a quadratic (hence cyclic) extension, this holds if and only if $\alpha^*\alpha$ is a norm in each $(K_0)_{v_0}$ from K_{v_0}, v_0 being any place of K_0, and K_{v_0} being the direct product of the completions of K at all places of K lying over v_0. If v_0 is

infinite and $\sigma_i : K_0 \to \mathbf{R}$ is the corresponding imbedding, $D \otimes_{K_0} \mathbf{R} = D \otimes_K (K \otimes_{K_0} \mathbf{R}) \simeq D \otimes_K \mathbf{C} \simeq M_d(\mathbf{C})$ and * extends to a map of $M_d(\mathbf{C})$ onto itself of the form $X^* = A \bar{X}^t A^{-1}$, $A \in GL(d, \mathbf{C})$. Hence $X^{**} = A.\bar{A}^{t-1}.X.\bar{A}^t.A^{-1}$, so that the image of α in $D \otimes_{K_0} \mathbf{R}$ is $\lambda A.\bar{A}^{t-1}$ for some $\lambda \in \mathbf{C}^*$, and $\alpha^*\alpha$ has for image $|\lambda|^2$ which is a norm from $\mathbf{C}$. Thus, it suffices to look at the Archimedean v_0. Again, if there are two extensions of v_0 to K, K_{v_0} is the direct product of two copies of $(K_0)_{v_0}$ as a $(K_0)_{v_0}$-algebra, so that the norm condition is vacuous.

Thus, we are left with the case of a v of K such that $\sigma v = v$. In this case, $\mathrm{Inv}_v(D) = 0$ or $\frac{1}{2}$ by (A). If $\mathrm{Inv}_v(D) = 0$, $D \otimes_K K_v$ is a matrix algebra over K_v and $A \longmapsto \sigma(A)^t$ is an involution of $D \otimes_K K_v$ inducing σ on K_v, so that, by the previous reasoning applied in the local case, $\alpha^*\alpha$ is a norm. Suppose now that $\mathrm{Inv}_v(D) = \frac{1}{2}$, so that $D_v = D \otimes_K K_v$ is a matrix algebra over the quaternion division algebra Q on K_v. Since σ induces the identity on $\mathrm{Br}(K_v)$ (see the theorem above), condition (A) gives us a σ-linear map $Q \to Q$, $X \longmapsto \hat{X}$, such that $\widehat{(XY)} = \hat{Y}\hat{X}$. If we put $\hat{\hat{X}} = \beta X \beta^{-1}$ for some $\beta \in Q$ and $X^* = A \hat{X}^t A^{-1}$ for all $X \in D_v$ and some $A \in D_v$, we see that upto a factor which is an element of the center, α equals $A \hat{A}^{t-1}\beta$, and $\alpha^*\alpha$ differs from

$$A.(A\hat{A}^{t-1}\beta)^{\wedge t}.A^{-1}(A\hat{A}^{t-1}\beta) = A(\hat{\beta}\hat{\hat{A}}^{-1}\hat{A}^t)\hat{A}^{t-1}\beta$$

$$= A.\hat{\beta}\hat{\hat{A}}^{-1}.\beta = \hat{\beta}\beta$$

by a factor in $\mathrm{Nm}_{K_v/K_{0v}}(K_v^*)$. Hence $\alpha^*\alpha$ is a norm in K_{0v} if and only if $\hat{\beta}\beta$ is, hence if and only if Q admits an involution inducing σ on K_v. Suppose $'$ is such an involution. Then we have (by the functoriality of trace) that $\mathrm{Tr}\, x' = \sigma(\mathrm{Tr}\, x)$, so that if i: $Q \to Q$ is the canonical involution of Q, $i(x') = i(x)'$. Thus $x \overset{\phi}{\longmapsto} i(x')$ is an automorphism ϕ of order two of Q inducing σ on K. If we put $Q_0 = \{x \in Q \mid \phi(x) = x\}$, Q_0 is a K_0-subalgebra of Q and $K_v \otimes_{K_{0v}} Q_0 \to Q$ is an isomorphism. But now, Q_0 is of rank four over K_{0v}, hence a quaternion algebra, and since $\mathrm{Br}(K_{0v}) \to \mathrm{Br}(K_v)$ is, by

means of the canonical isomorphisms with $\mathbf{Q}/\mathbf{Z}$, nothing but multiplication by 2, $Q = Q_0 \otimes_{K_{0v}} K_v$ is a matrix algebra over K_v, which is a contradiction.

Thus, if K_0 is a totally real field, K a purely imaginary quadratic extension of K and D a central division algebra on K, the necessary and sufficient condition for the existence of an involution of D inducing the non-trivial automorphism σ of K over K_0 is that besides (A), we also have

$$\mathrm{Inv}_v(D) = 0 \text{ if } \sigma v = v. \tag{B}$$

Step IV. Suppose then that (A) and (B) hold and let $x \longmapsto x^*$ be an involution. We shall then show that there are positive involutions too and we will classify them. For this, choose an isomorphism

$$D \otimes_{\mathbf{Q}} \mathbf{R} \xrightarrow{\sim} \overbrace{M_d(\mathbf{C}) \times M_d(\mathbf{C}) \times \ldots \times M_d(\mathbf{C})}^{e_0 \times}.$$

Then the given involution has an extension to the right side given by $(X_1, X_2, \ldots, X_{e_0}) \longmapsto (A_1 \bar{X}_1^t A_1^{-1}, \ldots, A_{e_0} \bar{X}_{e_0}^t A_{e_0}^{-1})$ with $\bar{A}_i^t = \eta_i A_i$, $\eta_i \in \mathbf{C}^*$, $A_i \in GL(d, \mathbf{C})$. We must have $|\eta_i| = 1$, and on replacing A_i by a scalar multiple, we may assume $\eta_i = 1$, so that $\bar{A}_i^t = A_i$. Hence, if $A = (A_1, \ldots, A_{e_0})$, we have $A^* = A$. The set of $A \in D \otimes_{\mathbf{Q}} \mathbf{R}$ with $A^* = A$ is of the form $V \otimes_{\mathbf{Q}} \mathbf{R}$ where V is a $\mathbf{Q}$-subspace of D, so that we can find an $\alpha \in V$ such that $\alpha \otimes 1$ is arbitrarily close to $A \in D \otimes_{\mathbf{Q}} \mathbf{R}$. The map $x \longmapsto x' = \alpha^{-1}x^*\alpha$ is again an involution of D whose extension to $M_d(\mathbf{C}) \times \ldots \times M_d(\mathbf{C})$ is arbitrarily close to $(X_1, \ldots, X_{e_0}) \longmapsto (\bar{X}_1^t, \ldots, \bar{X}_{e_0}^t)$. Hence for α a good enough approximation to A, $\mathrm{Tr}_{D/\mathbf{Q}}(x.x') > 0$ if $x \neq 0$, $x \in D$. On $M_d(\mathbf{C}) \times \ldots \times M_d(\mathbf{C})$, this involution is of the form

$$(X_1, \ldots, X_{e_0}) \longmapsto (A_1 \bar{X}_1^t A_1^{-1}, \ldots, A_{e_0} \bar{X}_{e_0}^t A_{e_0}^{-1}),$$

with A_i hermitian and close to I, so that the A_i are positive definite. Let B_i be a positive definite square root of A_i. Modifying the chosen isomorphism $D \otimes_{\mathbf{Q}} \mathbf{R} \xrightarrow{\sim} M_d(\mathbf{C}) \times \ldots \times M_d(\mathbf{C})$ by the inner automorphism given by $B = (B_1, \ldots, B_{e_0})$, we see that we

may assume that the extension of the involution to $M_d(\mathbf{C}) \times \ldots \times M_d(\mathbf{C})$ is the standard one

$$(X_1, \ldots, X_{e_0}) \longmapsto (\overline{X}_1^t, \ldots, \overline{X}_{e_0}^t),$$

which is certainly positive.

Thus, when (A) and (B) hold, we have found one positive involution on D and an isomorphism $D \otimes_{\mathbf{Q}} \mathbf{R} \xrightarrow{\sim} M_d(\mathbf{C}) \times \ldots \times M_d(\mathbf{C})$ such that the involution goes over into the standard one written above. Suppose $*$ is any other positive involution, so that $x^* = \alpha x' \alpha^{-1}$, $\alpha' = \lambda\alpha$ for some $\lambda \in K$. Since $\lambda.\lambda' = \mathrm{Nm}_{K/K_0}\lambda = 1$, we can write $\lambda = \dfrac{\sigma\mu}{\mu}$ for some $\mu \in K$, and when α is replaced by $\mu\alpha$, the involution is unchanged whereas the new α satisfies $\alpha' = \alpha$. Hence α goes over into $(A_1, \ldots, A_{e_0}) \in M_d(\mathbf{C}) \times \ldots \times M_d(\mathbf{C})$ with A_i hermitian. Positivity of $\mathrm{Tr}(x\,x^*)$ gives us the condition that $\mathrm{Tr}(X\,A_i\,\overline{X}^t\,A_i^{-1}) > 0$ for $X \in M_d(\mathbf{C})$, or equivalently, for some unitary U and any $X \in M_d(\mathbf{C})$,

$$\mathrm{Tr}(UXU^{-1}A_iU\overline{X}^tU^{-1}A_i^{-1}) = \mathrm{Tr}(XU^{-1}A_iU\overline{X}^tU^{-1}A_i^{-1}U) > 0.$$

Choose U so that $U^{-1}A_iU$ is real diagonal:

$$U^{-1}A_iU = \begin{bmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_d \end{bmatrix} = D_i.$$

We must then have $\mathrm{Tr}(X\,D\,\overline{X}^t\,D^{-1}) > 0$ for all $X \in M_d(\mathbf{C})$. But if $X = (x_{ij})$,

$$\mathrm{Tr}(X\,D\overline{X}^tD^{-1}) = \sum_{j,k=1}^{d} |x_{jk}|^2 \frac{\lambda_j}{\lambda_k},$$

so the condition is that D is positive definite or negative definite. Since we may replace α by $-\alpha$, this proves that all positive involutions are of the form $x \longmapsto \alpha x' \alpha^{-1}$ where the hermitian matrices A_i are positive definite.

Summarizing, we have

THEOREM 2. *Let D be a division algebra of finite rank over $\mathbf{Q}$ with an involution $'$ such that $\mathrm{Tr}_{D/\mathbf{Q}}(xx') > 0$ for $x \in D$, $x \neq 0$. Let K be the center of D and K_0 the subfield of elements of K fixed by $'$. Then $(D, ')$ is one of the following types.*

TYPE I. $D = K = K_0$ is a totally real algebraic number field and the involution is the identity.

TYPE II. $K = K_0$ is a totally real algebraic number field and D a quaternion division algebra over K (i.e. a central division algebra of rank 4 on K) such that for any imbedding $\sigma: K \to \mathbf{R}$,

$$\mathbf{R}_{(\sigma)} \otimes_K D \simeq M_2(\mathbf{R}).$$

Let $x^* = \mathrm{Tr}\ x - x$ be the standard involution of D and $a \in D$ such that $a^2 \in K$ and a^2 is totally negative. Then the involution is of the form $x' = a\,x^*a^{-1}$, and conversely, any such map is a positive involution. For any such involution, we can choose an isomorphism

$$\mathbf{R} \otimes_{\mathbf{Q}} D \xrightarrow{\sim} M_2(\mathbf{R}) \times \ldots \times M_2(\mathbf{R}) \ (e = [K: \mathbf{Q}] \text{ factors})$$

such that the involution extended to the right side by $\mathbf{R}$-linearity is given by $(X_1, \ldots, X_e) \to (X_1^t, \ldots, X_e^t)$.

TYPE III. $K = K_0$ is a totally real algebraic number field and D a quaternion division algebra over K such that for any imbedding $\sigma: K \to \mathbf{R}$,

$$\mathbf{R}_{(\sigma)} \otimes_K D \simeq \mathbf{K},$$

where $\mathbf{K}$ is the standard algebra of quaternions on $\mathbf{R}$. In this case the involution $'$ is the standard one, $x' = \mathrm{Tr}_{D/K}x - x$, and there is an isomorphism

$$\mathbf{R} \otimes_{\mathbf{Q}} D \xrightarrow{\sim} \mathbf{K} \times \ldots \times \mathbf{K},$$

carrying the involution into the product of the standard involutions in each factor $\mathbf{K}$.

TYPE IV. K_0 is a totally real algebraic number field, K a totally imaginary quadratic extension of K_0 with conjugation σ over K_0. Then D is a division algebra with center K such that (i) if v is a finite place fixed by σ, $\mathrm{Inv}_v(D) = 0$, and (ii) for any finite place v of K, $\mathrm{Inv}_v(D) + \mathrm{Inv}_{\sigma v}(D) = 0$.

In this case, there exist totally positive involutions $x \longmapsto x'$ and isomorphisms

$$\mathbf{R} \otimes_{\mathbf{Q}} D \xrightarrow{\sim} M_d(\mathbf{C}) \times \ldots \times M_d(\mathbf{C})$$

which carry the involution into the standard involution $(X_1, \ldots, X_{e_0}) \longmapsto (\overline{X}_1^t, \ldots, \overline{X}_{e_0}^t)$. Given one such $'$, any other positive involution $*$ of D is of the form $x^* = a\, x'\, a^{-1}$ with $a \in D$, $a' = a$ and such that the image of $1 \otimes a$ by the above isomorphism is of the form $(A_1, \ldots, A_{e_0})$ with A_i hermitian positive definite.

The following table gives the numerical invariants in all four types, and also indicates the restrictions on these invariants when $D = \mathrm{End}^0 X$ where X is a simple g-dimensional abelian variety. The symbols e, e_0, and d have the same significance as before, and $S = \{x \in D \mid x' = x\}$ and $\eta = \dfrac{\dim_{\mathbf{Q}} S}{\dim_{\mathbf{Q}} D}$.

Type	e	d	η	Restriction in char 0 when $D = \mathrm{End}^0 X$, $\dim X = g$	Restriction in char $p > 0$ when $D = \mathrm{End}^0 X$ $\dim X = g$
I	e_0	1	1	$e \mid g$	$e \mid g$
II	e_0	2	$\frac{3}{4}$	$2e \mid g$	$2e \mid g$
III	e_0	2	$\frac{1}{4}$	$2e \mid g$	$e \mid g$
IV	$2e_0$	d	$\frac{1}{2}$	$e_0 d^2 \mid g$	$e_0 d \mid g$

Excepting the indicated restrictions, all the assertions contained in the table have been proved. As for the restrictions, they are immediate consequences of the three divisibility results established earlier, viz. (i) in char 0, $\dim D \mid 2 \dim X$, (ii) in char $p > 0$, $ed \mid 2 \dim X$, and (iii) if L is a subfield of D whose elements are fixed by the involution, $[L\colon \mathbf{Q}] \mid g$.

One might ask to what extent the conditions derived above on the endomorphism rings of a simple abelian variety are complete, that is, given a division algebra of one of the four types and an integer g fulfilling the restrictions imposed

above, whether there exists a simple abelian variety of dimension g having the given algebra as endomorphism algebra. In characteristic zero at least, the answer is known and is due to Albert. The result is that there always exists such an X, excepting when D is of type III or IV *and* the quotient $g/2e$ in the first case and $g/e_0 d^2$ in the second case is 1 or 2. Even in these exceptional cases, it is known what further restrictions ensure the existence of an X (cf. Shimura, [Sh], esp. §4). On the other hand, not much seems to be known in positive characteristics.

APPLICATION II. THE RIEMANN HYPOTHESIS.

We first prove the

PROPOSITION. *Let X be an abelian variety, $'$ the Rosati involution on* $\mathrm{End}^0 X$ *defined by some ample line bundle and* $\alpha \in \mathrm{End}\, X$ *such that* $\alpha' \alpha = a \in \mathbf{Z}$. *Let* $\omega_1, \ldots, \omega_{2g}$ *be the roots (in* $\mathbf{C}$*) of the characteristic polynomial P of α. Then the subalgebra* $\mathbf{Q}[\alpha] \subset \mathrm{End}\, X$ *generated by α is semi-simple, and*

(i) $|\omega_i|^2 = a$ *for all* i;

(ii) *the map* $\omega_i \to \dfrac{a}{\omega_i}$ *is a permutation of the roots* ω_i.

PROOF. Note that (ii) is an immediate consequence of (i) since $\dfrac{a}{\omega_i} = \overline{\omega}_i$ and P is an integral polynomial. Next, let $Q(X)$ be the minimal polynomial over $\mathbf{Q}$ of α (as an element in $\mathrm{End}\, X$). I claim that P and Q have the same complex roots. In fact, since P has integral coefficients, and $P(\alpha) = 0$, $Q \mid P$. But also P is the characteristic polynomial of $T_l(\alpha)$ in the matrix representation

$$T_l\colon \mathrm{End}(X) \longrightarrow \mathrm{End}(T_l X).$$

If $\omega \in \overline{\mathbf{Q}}_l$ (algebraic closure of $\mathbf{Q}_l$) is a root of P, then ω is an eigenvalue of $T_l(\alpha)$, hence $Q(\omega)$ is an eigenvalue of $T_l(Q(\alpha))$. But $T_l(Q(\alpha)) = 0$, so $Q(\omega) = 0$, i.e. all roots of P in $\overline{\mathbf{Q}}_l$ are roots of Q. Therefore $P \mid Q^n$ for some n, and P and Q have the same complex roots too.

The restriction S of the trace on End^0X to $\mathbf{Q}[\alpha]$ is a trace form on $\mathbf{Q}[\alpha]$ satisfying $S(X.X') > 0$ if $X \in \mathbf{Q}[\alpha]$, $X \neq 0$. Further, since α is invertible in End^0X and $\mathbf{Q}[\alpha]$ is finite-dimensional, it follows that $\alpha^{-1} \in \mathbf{Q}[\alpha]$. Hence $\alpha' = a/\alpha \in \mathbf{Q}[\alpha]$, so $\mathbf{Q}[\alpha]$ is stable for the involution. If $\mathfrak{A} \subset \mathbf{Q}[\alpha]$ is any ideal in $\mathbf{Q}[\alpha]$, and $\mathfrak{b}$ is its orthogonal complement in $\mathbf{Q}[\alpha]$ for the quadratic form $S(X.X')$, $\mathfrak{b}$ is again an ideal and $\mathfrak{A} \cap \mathfrak{b} = (0)$, $\mathfrak{A} \oplus \mathfrak{b} = \mathbf{Q}[\alpha]$. Thus $\mathbf{Q}[\alpha]$ is semisimple, hence isomorphic to $K_1 \times K_2 \times \ldots \times K_p$ where K_i are algebraic number fields. The involution, being an automorphism of $\mathbf{Q}[\alpha]$, permutes the factors K_i. But since $S(X.X') > 0$ for every $X \neq 0$, the involution must take each K_i onto itself, and therefore S is a trace form on each K_i over $\mathbf{Q}$ with $S(X.X') > 0$ if $X \neq 0$. Hence each K_i is either totally real with identity involution or is a totally imaginary quadratic extension of a totally real subfield with complex conjugation for involution. Now, the roots ω of the minimal polynomial of α are precisely the images of α under the various imbeddings ϕ_j of the K_i in $\mathbf{C}$. Since $\phi_j(x') = \overline{\phi_j(x)}$ for all $x \in \mathbf{Q}[\alpha]$, it follows that

$$a = \phi_j(a) = \phi_j(\alpha'.\alpha) = |\phi_j(\alpha)|^2.$$

We shall apply this proposition to obtain a proof of the Riemann hypothesis on abelian varieties over finite fields. Let $\mathbf{F} = \mathbf{F}_q$ be a finite field with $q = p^f$ elements, and X_0 a scheme of finite type over $\mathbf{F}$. (We do not consider X_0 as a variety whose points are geometric points with values in an algebraically closed field, but as a scheme in Grothendieck's sense.) We define the *Frobenius morphism on* X_0, $\pi_0: X_0 \to X_0$, to be the identity on the underlying space together with the homomorphism $\mathcal{O}_{X_0} \to \mathcal{O}_{X_0}$ of structure sheaves given by $f \longmapsto f^q$. Note that this is a homomorphism of sheaves of $\mathbf{F}$-algebras since $\lambda^q = \lambda$ for $\lambda \in \mathbf{F}$, so π_0 is a morphism over Spec $\mathbf{F}$. Now let k be the algebraic closure of $\mathbf{F}_q$, and let X be the k-scheme $X = k \otimes_{\mathbf{F}} X_0$. The morphism $\pi: X \to X$ obtained from π_0 by base extension is called the *Frobenius morphism on* X, relative to $\mathbf{F}$ and to X_0. Let us see what this looks like on the geometric (or closed) points of X. Suppose that $X_0 = \mathrm{Spec}\ A$, where

$A = \mathbf{F}[X_1, \ldots, X_m]/\mathfrak{A}$, so that X_0 is embedded as a closed subscheme in $\mathbf{A}_{\mathbf{F}}^m$, and the closed points of X can be considered as elements of the set k^m. The morphism π_0 is defined by the homomorphism of $\mathbf{F}$-algebras $A \to A$ sending $\overline{X_i}$ into $\overline{X_i^q}$, so that if $(x_1, \ldots, x_m)$ is a geometric point of X, π maps it into the point $(x_1^q, \ldots, x_m^q)$. In particular, a point $(x_1, \ldots, x_m)$ is fixed by π^n if and only if $x_i^{q^n} = x_i$, i.e. if and only if x_i is a rational point over the field $\mathbf{F}_{q^n}$ with q^n elements. Further, the Frobenius morphism has the functorial property that if $f: X_0 \to Y_0$ is a morphism of $\mathbf{F}$-schemes and π_{0,X_0} and π_{0,Y_0} are the Frobenius maps of X_0 and Y_0, respectively, $\pi_{0,Y_0} \circ f = f \circ \pi_{0,X_0}$. Finally, it is clear that the map induced on tangent spaces by π at any point of X is 0, since $D(f^q) = 0$ for any derivation D of a ring A of characteristic p and $f \in A$.

THEOREM 3. (Lang.) *Let X_0 be a scheme over $\mathbf{F}_q$ such that $X = k \otimes_{\mathbf{F}} X_0$ is an abelian variety. Then X_0 has at least one point rational over $\mathbf{F}_q$.*

PROOF. If π is the Frobenius morphism, then π must have the form $\pi(x) = x_0 + f(x)$ for some closed point $x_0 \in X$ and some endomorphism f of X. Then $1 - f$ is an endomorphism of X. Since π and hence f induce the zero map on the tangent space at 0, $1 - f$ induces the identity on this tangent space. Therefore $\ker(1-f)$ is 0-dimensional and $1 - f$ is surjective. Then if $(1-f)(x_1) = x_0$, it follows that $x_1 = x_0 + f(x_1) = \pi(x_1)$, hence x_1 is rational over $\mathbf{F}_q$.

Therefore, if X is an abelian variety, by choosing an appropriate origin $0 \in X$, we can always assume that 0 is $\mathbf{F}$-rational. Then each π^n fixes 0 and is therefore an endomorphism of X. Moreover, $1 - \pi^n$ induces the identity on the tangent space at 0, so it is also a separable endomorphism. Hence we obtain:

$$N_n \underset{\text{def}}{=} \text{Number of } \mathbf{F}_{q^n}\text{-rational points of } X = \#(\mathrm{Ker}(1 - \pi^n)) = \deg(1 - \pi^n).$$

But if $\omega_1, \ldots, \omega_{2g}$ are the roots of the characteristic polynomial of π, then the characteristic polynomial $P_n(t)$ of π^n, for all n, is $\prod_{i=1}^{2g}(t - \omega_i^n)$. Since $\deg(1 - \pi^n) = P_n(1)$, it follows that

$$N_n = \prod_{i=1}^{2g} (1 - \omega_i^n).$$

We now wish to show $|\omega_i| = \sqrt{q}$: this is the Riemann hypothesis. Since it suffices to prove that $|\omega_i^m| = \sqrt{q^m}$ for some m, we may replace $\mathbf{F}_q$ by $\mathbf{F}_{q^m}$, X_0 by $\mathbf{F}_{q^m} \otimes_{\mathbf{F}} X_0$ and π by π^m if necessary. By doing this, we can assume that there is a line bundle L_0 on X_0 such that $L = k \otimes_{\mathbf{F}} L_0$ is ample on X (since any line bundle on X is of this form for suitably large m). Denoting by $'$ the Rosati involution with respect to L, we shall prove that

(i) $$\pi' \circ \pi = q,$$

so that the proposition applies. But by the definition of $'$ this means that

(ii) $$\hat{\pi}(\phi_L(\pi(x))) = q\phi_L(x), \quad \text{all } x \in X.$$

But π_0 acts on $\mathcal{O}_{X_0}$ by $f \longmapsto f^q$, so it follows that $\pi_0^* L_0 \simeq L_0^q$. Therefore $\pi^* L \simeq L^q$ and

(iii) $$\begin{aligned} \pi^*(T_{\pi x}^* L \otimes L^{-1}) &\simeq T_x^* \pi^* L \otimes (\pi^* L)^{-1} \\ &\simeq (T_x^* L \otimes L^{-1})^{\otimes q}. \end{aligned}$$

Since the line bundle on the left represents $\hat{\pi}(\phi_L(\pi(x)))$ and the line bundle on the right represents $q.\phi_L(x)$, (ii) and hence (i) are correct.

We summarize our conclusions in

THEOREM 4. (Weil.) *Let X_0 be a scheme over $\mathbf{F}_q$ such that $X = k \otimes_{\mathbf{F}} X_0$ is an abelian variety. Let N_n = the number of points of X rational over $\mathbf{F}_{q^n}$. Then*

$$N_n = \prod_{i=1}^{2g} (\omega_i^{2g^n} - 1)$$

where $\omega_i \in \mathbf{C}$ and they satisfy

(i) $|\omega_i| = \sqrt{q}$,

(ii) $\omega_{ni} = q/\omega_i$ *for some permutation* π.

COROLLARY. *For some constant C, $|N_n - q^{ng}| < C.\, q^{n(g-\frac{1}{2})}$ for all n.*

Another application of the proposition is

THEOREM 5. (Serre.) *For any $n \geqslant 3$, and any L ample on an abelian variety X, the restriction homomorphism*

$$\left\{ \alpha \in \operatorname{Aut} X \,\middle|\, \alpha^* L \simeq L \otimes \begin{pmatrix} \text{something} \\ \text{in } \operatorname{Pic}^0 X \end{pmatrix} \right\} \longrightarrow \operatorname{Aut}(X_n)$$

is injective (here X_n = scheme-theoretic kernel of n_X).

PROOF. If $\alpha^* L \simeq L \otimes \begin{pmatrix} \text{something} \\ \text{in } \operatorname{Pic}^0 X \end{pmatrix}$, then $\phi_{\alpha^* L} = \phi_L$, hence $\hat{\alpha} \circ \phi_L \circ \alpha = \phi_L$. This means that for the Rosati involution defined by L, $\alpha'\alpha = 1$. Hence by the proposition the roots of the characteristic polynomial of α are algebraic integers all of whose conjugates have absolute value 1, and hence are all roots of unity.

Suppose now that α restricts to the identity on some $X_n (n \geqslant 3)$. Then the restriction of $\alpha - 1$ to X_n is 0, so that $(\alpha - 1) = n\beta$ for some $\beta \in \operatorname{End} X$. We deduce that if ω is any characteristic root of α, $\omega - 1 = n\eta$ where η is an algebraic integer. We now have the

LEMMA. *If ω is a root of unity such that $\omega = 1 + n\eta$ where n is a rational integer $\geqslant 3$ and η an algebraic integer, then $\omega = 1$.*

PROOF. If not, by raising ω to a suitable power, we may assume that ω is a primitive p-th root of unity for a prime p. Taking norms over $\mathbf{Q}$ in the equation $\omega - 1 = n\eta$, we obtain

$$\prod_{i=1}^{p-1} (1 - \omega^i) = n^{p-1}.N,$$

where $N = (-1)^{p-1} \operatorname{Nm} \eta$ is a rational integer. But the left side is the derivative at $X = 1$ of $X^p - 1 = \prod_{i=0}^{p-1} (X - \omega^i)$, that is, p. Hence n^{p-1} divides p, which is impossible if $n \geqslant 3$.

Applying the lemma, we deduce that the characteristic roots of α are all 1, so that $1 - \alpha$ is nilpotent. But by the proposition, $\mathbf{Q}[\alpha]$ is semi-simple, so it has no nilpotent elements. Thus $\alpha = 1$.

APPLICATION III. STRUCTURE OF $NS^0(X)$.

Let X be an abelian variety and let $NS^0(X) = NS(X) \otimes \mathbf{Q}$. As in § 20, if we fix an ample L on X, then we can identify

$$NS^0(X) \xrightarrow[\rho]{\sim} \{\alpha \in \mathrm{End}^0 X \mid \alpha' = \alpha\}.$$

In particular, $NS^0(X)$ has a natural structure of Jordan algebra over $\mathbf{Q}$ if we define

$$\alpha \circ \beta = \tfrac{1}{2}\rho^{-1}(\rho(\alpha)\rho(\beta) + \rho(\beta)\rho(\alpha)),\ \alpha, \beta \in NS^0(X),$$

using composition in $\mathrm{End}^0 X$. What can we say about this Jordan algebra? First of all, the fact that $\mathrm{Tr}(\rho(\alpha)^2) > 0$, all $\alpha \in NS^0(X)$, $\alpha \neq 0$, implies immediately that $NS^0(X)$ is *formally real*, i.e.

$$\sum_{i=1}^{n} \alpha_i \circ \alpha_i = 0 \Rightarrow \alpha_1 = \ldots = \alpha_n = 0$$

(cf. Braun, Koecher, [B-K] Ch. 11, § 3). Now the formally real Jordan algebras over $\mathbf{R}$ have been classified: cf. Braun, Koecher, Ch. 11, § 5. In our case, we do not get all possible such algebras by forming $NS^0(X) \otimes \mathbf{R}$. In fact, we have

THEOREM 6. *$NS^0(X) \otimes \mathbf{R}$ is isomorphic to a product of Jordan algebras of the types:*

$\mathscr{H}_r(\mathbf{R})$ $= r \times r$ *symmetric real matrices*

$\mathscr{H}_r(\mathbf{C})$ $= r \times r$ *Hermitian complex matrices*

$\mathscr{H}_r(\mathbf{K})$ $= r \times r$ *Hermitian quaternionic matrices, i.e.* ${}^t\overline{X} = X$, *where* $x \to \bar{x}$ *is the standard involution on* $\mathbf{K}$.

PROOF. Decompose $\mathrm{End}^0(X) \otimes \mathbf{R}$ into a product of copies of $M_n(\mathbf{R})$, $M_n(\mathbf{C})$ and $M_n(\mathbf{K})$. Then $NS^0(X) \otimes \mathbf{R}$ is isomorphic to the set of fixed points here under a positive involution. But it is easy to check that every such involution (a) fixes each of the factors $M_n(K)$, $K = \mathbf{R}$, $\mathbf{C}$ or $\mathbf{K}$, and (b) by inner automorphism of each factor, can be put in the standard form $X \to {}^t\overline{X}$. [Cf. the proof of Theorem 2, Step IV, for the case $K = \mathbf{C}$; the other cases are analogous. One checks first that every positive involution of $M_n(K)$ is of the form $X \longmapsto A \cdot {}^t\overline{X} \cdot A^{-1}$ where ${}^t\bar{A} = A$. One then

checks that $A = U \cdot D \cdot U^{-1}$ where D is diagonal with real entries either all positive or all negative and ${}^t\overline{U} = U^{-1}$. Finally, solve $\pm D = E^2$ and use the inner automorphism defined by UEU^{-1} to put the involution in standard form.]

Fix isomorphisms ϕ and ψ:

$$\begin{array}{lcl} \text{(I)} \quad \mathrm{End}^0(X) \otimes \mathbf{R} & \xrightarrow[\phi]{\sim} & \prod M_{r_i}(\mathbf{R}) \times \prod M_{s_i}(\mathbf{C}) \times \prod M_{t_i}(\mathbf{K}) \\ \uparrow \rho & & \cup \\ NS^0(X) \otimes \mathbf{R} & \xrightarrow[\psi]{\sim} & \prod \mathscr{H}_{r_i}(\mathbf{R}) \times \prod \mathscr{H}_{s_i}(\mathbf{C}) \times \prod \mathscr{H}_{t_i}(\mathbf{K}). \end{array}$$

What happens to the polynomial function $\chi\colon NS^0(X) \otimes \mathbf{R} \to \mathbf{R}$? For any $x \in \mathrm{End}^0(X) \otimes \mathbf{R}$, let $\phi_{i,1}(x)$, $\phi_{i,2}(x)$, $\phi_{i,3}(x)$ denote the components of $\phi(x)$ in the above decomposition. Then we know that the function "degree" can be written

$$\text{(II)} \quad \deg(x) = \prod \det(\phi_{i,1}x)^{a_i} \cdot \prod |\det(\phi_{i,2}x)|^{2b_i} \cdot \prod \mathrm{Nm}(\phi_{i,3}x)^{c_i}$$

where $\mathrm{Nm}\colon M_t(\mathbf{K}) \to \mathbf{R}$ is the reduced norm (the multiplicative polynomial of degree $2t$). Now on $NS(X)$, $\deg(\rho x) = \alpha \cdot \chi(x)^2$ for some constant α. It follows that the a_i are even and that the function χ can be written

$$\text{(III)} \quad \chi(x) = \mathrm{const.} \prod \det(\psi_{i,1}x)^{a_i/2} \cdot \prod \det(\psi_{i,2}x)^{b_i} \cdot \prod \mathrm{HNm}(\psi_{i,3}x)^{c_i}$$

all $x \in NS^0(X) \otimes \mathbf{R}$. Note that $\psi_{i,2}(x)$ is Hermitian, so its complex determinant is real. Here "HNm" is the "Haupt norm" of Braun-Koecher (Ch. 2. §4), a polynomial function of degree t from $\mathscr{H}_t(\mathbf{K})$ to $\mathbf{R}$. If $\lambda_0 \in NS^0(X) \otimes \mathbf{R}$ is the point defined by the ample L on X used to set up ρ, then $\rho(\lambda_0) = 1$, so $\psi_{i,j}(\lambda_0) = I$, so the constant in the above formula is $\chi(\lambda_0)$. Using the results of §16, it follows finally that:

(IV) If $\chi(x) \neq 0$, then

$$i(x) = \sum \frac{a_i}{2} \begin{pmatrix} \#\text{ neg. eigenvalues} \\ \text{of } \psi_{i,1}\,x \end{pmatrix} + \sum b_i \begin{pmatrix} \#\text{ neg. eigenvalues} \\ \text{of } \psi_{i,2}\,x \end{pmatrix} + \sum c_i \begin{pmatrix} \#\text{ neg. eigenvalues} \\ \text{of } \psi_{i,3}\,x \end{pmatrix}.$$

(The eigenvalues of a quaternionic Hermitian matrix H are defined as the entries of a diagonal matrix D such that $H = U \cdot D \cdot U^{-1}$, and ${}^t\overline{U} = U^{-1}$.) Since ample line bundles L are characterized by $\chi(L) \neq 0$, $i(L) = 0$, it follows from (III) and (IV) that the images of the ample line bundles in $NS(X)$ are exactly the totally positive elements of the formally real Jordan algebra $NS^0(X) \otimes \mathbf{R}$.

22. Examples.

FIRST EXAMPLE: ABELIAN VARIETIES OF CM-TYPE OVER $\mathbf{C}$.

Let X be a simple g-dimensional abelian variety, $D = \mathrm{End}^0(X)$, $K =$ center of D, $d^2 = [D:K]$ and $e = [K:\mathbf{Q}]$. Recall that $ed \mid 2g$ and that we have called X of *CM*-type if $ed = 2g$. We wish to classify these when $k = \mathbf{C}$. A glance at the table in §20 giving the types of division algebras D tells us that we must have $K = D$, K a totally imaginary quadratic extension of a totally real field K_0 of degree g over $\mathbf{Q}$.

We pose the problem a little differently. Suppose we are given a totally real number field K_0 of degree g over $\mathbf{Q}$ and a totally imaginary quadratic extension K of K_0. We consider all pairs (i, X) where X is an abelian variety over $\mathbf{C}$ of dimension g and $i: K \to \mathrm{End}^0 X$ is an imbedding of the field K in the ring $\mathrm{End}^0 X$. We define two such pairs (i, X) and (j, Y) to be equivalent if there is an isogeny $\alpha: X \to Y$ such that if $\tilde{\alpha}: \mathrm{End}^0 X \xrightarrow{\sim} \mathrm{End}^0 Y$ is the induced isomorphism, we have $\tilde{\alpha} \circ i = j$. It is easily checked that this is an equivalence relation. Our object is to exhibit a complete set of representatives for the equivalence classes.

Let (i,X) be any such pair, V the tangent space of X at 0 and U the kernel of the exponential map from V to X, so that we have a natural isomorphism $V/U \xrightarrow{\sim} X$. Then $\mathrm{End}\, X$ acts faithfully as a ring of $\mathbf{C}$-endomorphisms of the vector space V, leaving U stable. Thus, if we put $i^{-1}(\mathrm{End}\, X) = A \subset K$, A is an order (i.e. a finitely generated subring of maximal rank) in K and U becomes an A-module. Thus, $\mathbf{Q}.U \subset V$ becomes a vector space over $\mathbf{Q} \otimes_{\mathbf{Z}} A = K$, and since both K and $\mathbf{Q}.U$ are of dimension $2g$ over $\mathbf{Q}$, $\mathbf{Q}.U$ is a one-dimensional K-vector space. Hence, if we choose a non-zero element $u_0 \in U$, the map $\phi: A \to U$ defined by $a \longmapsto a.u_0$ is an injection of A into U, such that the index $[U:\phi(A)] < +\infty$. Changing X by an isogeny, we can first shrink U so that $U = \phi(A)$, and then increase U so that $U = \phi(A_0)$, $A_0 =$ ring of integers in K. Next, the map ϕ extends to an $\mathbf{R}$-linear map which we still denote by ϕ:

$$\mathbf{R} \otimes_{\mathbf{Q}} K = \mathbf{R} \otimes_{\mathbf{Z}} A_0 \xrightarrow{\phi} \mathbf{R} \otimes_{\mathbf{Z}} U = V.$$

It follows that ϕ defines an isomorphism between the *real* tori:

$$(\mathbf{R} \otimes_{\mathbf{Q}} K)/A_0 \xrightarrow{\approx} V/U = X.$$

Note that if $a \in A_0$, then this isomorphism has been set up exactly so that the endomorphism $i(a): X \to X$ corresponds to multiplication by $1 \otimes a$ in $\mathbf{R} \otimes_{\mathbf{Q}} K$.

Next, let Φ denote the complex structure on the real vector space $\mathbf{R} \otimes_{\mathbf{Q}} K$ obtained by pulling back the complex structure on V via ϕ. Since multiplication by $1 \otimes a$ in $\mathbf{R} \otimes_{\mathbf{Q}} K (a \in A_0)$ goes over via ϕ to a complex-linear map from V to V, it follows that in the complex structure Φ, multiplication by $1 \otimes a$ is complex-linear too. In other words, Φ actually makes the $\mathbf{R}$-algebra $\mathbf{R} \otimes_{\mathbf{Q}} K$ into a $\mathbf{C}$-algebra as well as a $\mathbf{C}$-vector space. We now invert this whole construction.

DEFINITION. *If K is as above, $A_0 =$ integers in K, and Φ is a structure of $\mathbf{C}$-algebra on $\mathbf{R} \otimes_{\mathbf{Q}} K$, then let*

$$X(K, \Phi) = \textit{the complex torus } \mathbf{R} \otimes_{\mathbf{Q}} K / A_0,$$

and let $i_\Phi : A_0 \to \mathrm{Hom}_{\substack{\text{complex} \\ \text{tori}}}(X(K,\Phi), X(K,\Phi))$ be given by $i_\Phi(a) =$ map induced by mult. by $1 \otimes a$.

We have shown that for given K as above, and any pair (i, X), there is a structure Φ of complex algebra on the real algebra $\mathbf{R} \otimes_{\mathbf{Q}} K$ such that (i, X) is equivalent to $(i_\Phi, X(K, \Phi))$. Our next aim is to show that (i) for any structure Φ of complex algebra on $\mathbf{R} \otimes_{\mathbf{Q}} K$, $X(K, \Phi) = \mathbf{R} \otimes_{\mathbf{Q}} K / 1 \otimes A_0$ is an abelian variety, and (ii) for

different complex structures Φ_1 and Φ_2 on $\mathbf{R}\otimes_{\mathbf{Q}}K$, $(i_{\Phi_1}, X(K,\Phi_1))$ and $(i_{\Phi_2}, X(K,\Phi_2))$ are not equivalent.

To prove (i), let us look more closely at a structure Φ of complex algebra on $\mathbf{R}\otimes_{\mathbf{Q}}K$. Giving such a Φ is equivalent to giving a homomorphism $\tilde{\Phi}$ of $\mathbf{R}$-algebras, $\tilde{\Phi}\colon \mathbf{C} \to \mathbf{R}\otimes_{\mathbf{Q}}K$. Now, if $\sigma_i (1 \leqslant i \leqslant g)$ are the distinct embeddings of K_0 in $\mathbf{R}$, we have an isomorphism of $\mathbf{R}$-algebras

$$\mathbf{R}\otimes_{\mathbf{Q}}K \xrightarrow{\sim} (\mathbf{R}_{(1)}\otimes_{K_0}K) \times (\mathbf{R}_{(2)}\otimes_{K_0}K) \times \ldots \times (\mathbf{R}_{(g)}\otimes_{K_0}K),$$

$$\lambda\otimes\alpha \longmapsto (\lambda\otimes\alpha,\ \lambda\otimes\alpha,\ \ldots,\ \lambda\otimes\alpha),$$

where $\mathbf{R}_{(i)}$ is $\mathbf{R}$ considered as a K_0-algebra through σ_i. Thus, giving an $\mathbf{R}$-algebra homomorphism $\tilde{\Phi}\colon \mathbf{C}\to\mathbf{R}\otimes_{\mathbf{Q}}K$ is in turn equivalent to giving $\mathbf{R}$-algebra *isomorphisms* $\Phi_i\colon \mathbf{C}\xrightarrow{\sim}\mathbf{R}_{(i)}\otimes_{K_0}K$ for $1\leqslant i\leqslant g$. For each i, there are clearly two such possible $\mathbf{R}$-isomorphisms $\mathbf{C}\to\mathbf{R}_{(i)}\otimes_{K_0}K$. Thus, we see that there are exactly 2^g possible Φ on $\mathbf{R}\otimes_{\mathbf{Q}}K$, and each Φ is uniquely determined by giving the corresponding $\mathbf{R}$-isomorphisms $\Phi_i\colon \mathbf{C}\to\mathbf{R}_{(i)}\otimes_{K_0}K$ $(1\leqslant i\leqslant g)$. Let $\tau_i\colon \mathbf{R}_{(i)}\otimes_{K_0}K\to\mathbf{C}$ be the inverse of Φ_i, so that τ_i restricted to $K\simeq 1\otimes K\subset\mathbf{R}_{(i)}\otimes_{K_0}K$ is an imbedding of K in $\mathbf{C}$ extending the imbedding σ_i of K_0 in $\mathbf{R}$. We can choose an element $\alpha\in K$ such that $\alpha^2\in K_0$ and $\tau_i(\alpha)=i\beta_i$, $\beta_i\in\mathbf{R}$, $\beta_i>0$. In fact, if $K=K_0(\sqrt{\delta})$ then $\tau_i(\sqrt{\delta})=i\gamma_i$ with $\gamma_i\in\mathbf{R}^*$, and we can find $\eta\in K_0$ such that $\sigma_i(\eta)$ has the same sign as γ_i, and we can take $\alpha=\eta\sqrt{\delta}$. We may further assume α to be an algebraic integer. If $\tau_i(\alpha)=i\beta_i$ $(1\leqslant i\leqslant g)$, we define a Hermitian form H on $(\mathbf{R}\otimes_{\mathbf{Q}}K,\Phi)$ by putting

$$H(x,y)=2\sum_{i=1}^{g}\beta_i\,\tau_i(x)\,\overline{\tau_i(y)},\quad x,y\in\mathbf{R}\otimes_{\mathbf{Q}}K.$$

This form is clearly positive definite, and we shall show that $\operatorname{Im} H$ is integral on the lattice A_0. In fact, for $x, y\in A_0$, we have

$$\operatorname{Im} H(x,y)=-2\operatorname{Re}\sum_{i=1}^{g}i\beta_i\,\tau_i(x)\overline{\tau_i(y)}$$

$$=-2\sum_{i=1}^{g}\operatorname{Re}\,\tau_i(\alpha xy)$$

$$=-\sum_{i=1}^{g}(\tau_i(\alpha x\bar{y})+\bar{\tau}_i(\alpha x\bar{y}))$$

$$=-\operatorname{Tr}_{K/\mathbf{Q}}(\alpha x\bar{y})\in\mathbf{Z},$$

where for any $y\in K$, $\bar{y}$ denotes its conjugate over K_0. Thus, for any complex algebra structure Φ on $\mathbf{R}\otimes_{\mathbf{Q}}K$, and the lattice A_0 in it, H defined above is a Riemann form and $X(K,\Phi)$ is an abelian variety, proving assertion (i).

To prove (ii) suppose there is an equivalence of $(i_{\Phi_1}, X(K,\Phi_1))$ and $(i_{\Phi_2}, X(K,\Phi_2))$. Then we deduce an isomorphism of $\mathbf{C}$-vector spaces $\lambda\colon(\mathbf{R}\otimes_{\mathbf{Q}}K,\ \Phi_1)\xrightarrow{\sim}(\mathbf{R}\otimes_{\mathbf{Q}}K,\ \Phi_2)$ such that $\lambda(1\otimes K)=1\otimes K$ and λ is an isomorphism of K-modules. If $\lambda(1\otimes 1)=1\otimes x$, $x\in K^*$, by replacing λ by $(1\otimes x^{-1}).\lambda$ we may suppose further that $\lambda(1\otimes 1)=1\otimes 1$. Since λ is both K and $\mathbf{R}$-linear, we deduce that $\lambda(a\otimes x)=a\otimes x$, $a\in\mathbf{R}$, $x\in K$, so that λ is the identity. Since λ is $\mathbf{C}$-linear, we must have $\Phi_1=\Phi_2$, which establishes (ii).

We have therefore proved the

THEOREM. *Let K_0 be a totally real number field of degree g over $\mathbf{Q}$, and K a totally imaginary quadratic extension of K_0. Consider all pairs (X,i) where X is an abelian variety over $\mathbf{C}$ and $i\colon K\to \operatorname{End}^0 X$ an embedding, with the equivalence relation defined above.*

Then there are exactly 2^g equivalence classes, and as Φ runs through complex structures on $\mathbf{R}\otimes_{\mathbf{Q}}K$ which make $\mathbf{R}\otimes_{\mathbf{Q}}K$ a $\mathbf{C}$-algebra, the pairs $(X(K,\Phi), i_\Phi)$ give a complete system of representatives in the distinct equivalence classes.

REMARKS. (1) It is not true that $X(K,\Phi)$ is always simple. It can be shown that in order for $X(K,\Phi)$ to be simple, it is necessary and sufficient that there does not exist a proper subfield L of K satisfying the following conditions:

(i) L is a quadratic extension of $L\cap K_0$,

(ii) if Φ is given by the set of imbeddings $\tau_1, \ldots, \tau_g$ of K in $\mathbf{C}$, and if $\tau_i \mid L \cap K_0 = \tau_j \mid L \cap K_0$, then $\tau_i \mid L = \tau_j \mid L$.

If such an L exists, $X(K, \Phi)$ is isogenous to a power of $X(L, \Psi)$, where Ψ is given by $\{\tau_i \mid_{L \cap K_0}\}$.

(2) Let us specialize to the case of dimension one, that is, the case of elliptic curves over $\mathbf{C}$. If X is an elliptic curve over $\mathbf{C}$, either $\mathrm{End}^0 X = \mathbf{Q}$ or $\mathrm{End}^0 X = \mathbf{Q}(\sqrt{-d})$ for some square free $d \in \mathbf{Z}$, $d > 0$. Moreover, given any imaginary quadratic field $\mathbf{Q}(\sqrt{-d})$, there is an elliptic curve X with $\mathrm{End}^0 X \simeq \mathbf{Q}(\sqrt{-d})$, and upto an isogeny, $X \simeq \mathbf{C}/\{n + m\sqrt{-d} \mid n, m \in \mathbf{Z}\}$.

SECOND EXAMPLE: ELLIPTIC CURVES IN CHARACTERISTIC $p > 0$.

We begin with recalling some basic facts concerning abelian varieties of dimension one (or elliptic curves). These facts are immediate consequences of our general theory, as the reader may verify for himself.

Let X be an abelian variety of dimension one. We shall denote the divisor corresponding to a point P by $[P]$. Then, for any divisor D on X, we have $\chi(\mathcal{O}_X(D)) = \deg D$, and if further $\deg D > 0$, $\chi(\mathcal{O}_X(D)) = \dim H^0(\mathcal{O}_X(D))$ and $H^1(\mathcal{O}_X(D)) = (0)$. A divisor D belongs to $\mathrm{Pic}^0 X$ if and only if $\deg D = 0$. A divisor $D = \Sigma n_i [P_i]$ of degree 0 is linearly equivalent to zero if and only if $\Sigma n_i P_i = 0$ on X. Any divisor D of degree $\geqslant 3$ is very ample.

Suppose now that the characteristic is either 0 or greater than 2. Let 0 be the identity element of the group X and let P_1, P_2, and P_3 be the points of order two on X. Since $\dim H^0(\mathcal{O}_X(2[0]) = 2$, we can choose a non-constant function x having a double pole at 0 and regular elsewhere. Subtracting a constant from x, we may assume $x(P_1) = 0$, and since the sum of the zeros with multiplicity is 0 and there are exactly two zeros, we deduce that P_1 is a double zero of x and there are no other zeros. Thus, by dividing by a constant, we may assume that $x(P_2) = 1$ and $x(P_3) = \lambda \in k^*$. By applying the above argument to $x - 1$, we deduce that $\lambda \neq 0, 1$. Since $H^0(\mathcal{O}_X(3[0]))$ is of dimension 3, we can find a function y having a triple pole at 0 and regular elsewhere. By subtracting a suitable linear combination

$ax+b$ from y, we may assume that $y(P_1) = y(P_2) = 0$, and since the number of zeros is 3 (taking multiplicity into account) and the sum of the zeros is 0, we deduce that y has simple zeros at P_1, P_2 and $P_3 = -P_1 - P_2$. Both the functions y^2 and $x(x-1)(x-\lambda)$ have poles of order 6 at 0 and double zeros at P_1, P_2, and P_3 and no other zeros or poles anywhere, so that they differ by a non-zero scalar factor. Replacing y by a non-zero scalar multiple, we arrive at an equation

$$X_\lambda : y^2 = x(x-1)(x-\lambda) \qquad (N_p)$$

for $X - \{0\}$ in $\mathbf{A}^2(k)$. Conversely, the projective curve $y^2 t = x(x-t).(x-\lambda t)$ has no singularities and is of genus 1 for $\lambda \neq 0$ or 1, and hence defines an elliptic curve X_λ in $\mathbf{P}^2(k)$.

We wish to find all possible values of λ for which X_λ is of p-rank 0, for characteristics $p > 2$. We know that the p-rank is 0 if and only if the Frobenius map in $H^1(X, \mathcal{O})$ is trivial. The meromorphic form dx on X is regular in $X - \{0\}$ and vanishes at $P_1 = (0, 0)$, $P_2 = (1, 0)$ and $P_3 = (\lambda, 0)$ to the first order, and nowhere else, since $dx(P) = 0$ and $x(P) = \alpha$ implies that $x - \alpha$ vanishes to the second order at P, hence $2P$ must be 0. Thus, the form $\omega = dx/y$ is regular and nowhere vanishing in $X - \{0\}$. It follows that ω must be regular and non-vanishing at 0 also. If we put $U_0 = X - \{0\}$, $U_1 = X - \{P_1\}$, $\mathfrak{U} = (U_0, U_1)$ is an affine covering of X. A 1-cocycle for this covering is a regular function f in $U_0 \cap U_1 = X - \{0\} - \{P_1\}$, and this is a coboundary if and only if $f = g - h$ with g regular on U_0 and h regular on U_1. Consider the linear form on $C^1(\mathfrak{U}, \mathcal{O}) = \Gamma(U_0 \cap U_1, \mathcal{O})$ defined by $f \longmapsto \mathrm{Res}_{P_1}(f\omega)$. Since the residue at any point of a meromorphic form with a pole (of any order) at a single point of X and no other poles is zero by the residue theorem, we see that $\mathrm{Res}_{P_1}(f\omega) = 0$ if f is a coboundary. On the other hand, the function y/x is regular on $U_0 \cap U_1$ and has a simple pole at P_1, so that $\mathrm{Res}_{P_1}(y/x.\omega) \neq 0$. Since $\dim H^1(X, \mathcal{O}) = 1$, we deduce that the above linear form induces an isomorphism $H^1(X, \mathcal{O}) \xrightarrow{\sim} k$, and also that $y/x \in \Gamma(U_0 \cap U_1, \mathcal{O})$ defines a non-zero cohomology class in $H^1(X, \mathcal{O})$. Hence, the Frobenius map on $H^1(X, \mathcal{O})$ is trivial if and only if

$y^p/x^p \in \Gamma(U_0 \cap U_1, \mathcal{O})$ is a coboundary, hence if and only if $\mathrm{Res}_{P_1}\left(\frac{y^p}{x^p}\cdot\frac{dx}{y}\right) = 0$. Now,

$$\mathrm{Res}_{P_1}\left(\frac{y^p}{x^p}\cdot\frac{dx}{y}\right) = \mathrm{Res}_{P_1}\left(\frac{(y^2)^{\frac{(p-1)}{2}}}{x^{p-1}}\frac{dx}{x}\right)$$

$$= 2.\left\{\begin{array}{l}\text{coefficient of } x^{p-1} \text{ in}\\ (y^2)^{\frac{(p-1)}{2}} = x^{\frac{(p-1)}{2}}(x-1)^{\frac{(p-1)}{2}}(x-\lambda)^{\frac{(p-1)}{2}}\end{array}\right\}$$

$$= 2.\left\{\begin{array}{l}\text{coefficient of } x^{\frac{(p-1)}{2}} \text{ in}\\ (x-1)^{\frac{(p-1)}{2}}(x-\lambda)^{\frac{(p-1)}{2}}\end{array}\right\}$$

$$= \pm 2.\left\{\sum_{\nu=0}^{\frac{(p-1)}{2}}\binom{\frac{p-1}{2}}{\nu}^2.\ \lambda_\nu\right\} = \pm\, 2\,\Phi(\lambda),$$

where

$$\Phi(\lambda) = \sum_{\nu=0}^{\frac{p-1}{2}}\binom{\frac{p-1}{2}}{\nu}^2.\ \lambda^\nu.$$

Now, $\Phi(0)=$ coeff. of $x^{(p-1)/2}$ in $x^{(p-1)/2}(x-1)^{(p-1)/2}$, and $\Phi(1)=$ coeff. of $x^{(p-1)/2}$ in $(x-1)^{p-1} = \dfrac{x^p-1}{x-1} = 1 + x + \ldots + x^{p-1}$, so that $\Phi(0) \neq 0$, $\Phi(1) \neq 0$. Thus, every root of Φ defines an elliptic curve X_λ of p-rank 0, and these are the only elliptic curves of p-rank 0 upto isomorphism.

Let us call an elliptic curve in characteristic $p>0$ *supersingular* if its p-rank is 0. We have then shown that *in characteristic $p>2$, any supersingular curve is isomorphic to one of the X_λ where λ is a root of $\Phi(\lambda)$.* If $p=2$, it is not hard to see that there is exactly one supersingular elliptic curve, namely $y^2+y=x^3$. We omit this. Therefore, in any positive characteristic, there is one and there are only finitely many supersingular curves upto isomorphism.

We now study the algebra End^0X of an elliptic curve over a field of characteristic $p>0$. Let k be the algebraically closed field over which we work. We shall say that an abelian variety X over k is defined over a subfield k_0 of k if there is a scheme X_0 over k_0 such that $X \simeq k \otimes_{k_0} X$. We can then easily establish that there is a finite algebraic extension k_1 of k_0, a rational point 0 in $k_1 \otimes_{k_0} X_0 = X_1$ and a morphism $m_1: X_1 \times_{k_1} X_1 \to X_1$ over k_1 such that on base extension, we get (upto an isomorphism) the triplet $(X, 0, m)$. In future, when we speak of abelian varieties defined over various fields, we will assume that 0 is rational and m defined over this field. Another remark in this connection is that if $f: X \to Y$ is a *separable* isogeny and if either X or Y is defined over an algebraically closed subfield k_0 of k then f, X and Y are all defined over k_0. This is clear if we assume X defined over k_0, since Y is the quotient of X by its kernel which is a reduced finite subgroup of X, and all points of finite order in X are k_0-rational. Suppose on the other hand that Y is defined over k_0. By induction, we may assume f of prime degree l. If $l \neq p$, then there is a separable isogeny $g: Y \to X$, defined over k, such that $f\circ g: Y \to Y$ is l_Y, so that we are reduced to the first case. Suppose then that $l=p$, and let G be the infinitesimal part of p_Y, and $Y' = Y/G$. Then, G and Y' are defined over k_0. Then there is a separable isogeny $g: Y' \to X$, defined over k, such that the composite $Y \to Y' \to X \to Y$ is p_Y, so that we are reduced to the first case again.

THEOREM. (Deuring.) *Let X be an elliptic curve in characteristic $p>0$. We have the following equivalences.*

(a) *X cannot be defined over a finite field* $\iff \mathrm{End}^0X = \mathbf{Q}$.

(b) *Suppose X is defined over a finite field k_0. Then,*

(i) *End^0X is imaginary quadratic over $\mathbf{Q}$* $\iff$ *p-rank of X is 1* $\iff$ *$\pi^n \neq p_X^m$ for suitable integers n, m, where π is the Frobenius morphism over k_0.*

(ii) *If, however, the p-rank is 0, then End^0X is the (upto isomorphism, unique) quaternion division algebra $\mathbf{K}_{(p)}$ over $\mathbf{Q}$ which satisfies $\mathrm{Inv}_l\mathbf{K}_{(p)} = 0$ if l is finite and $\neq p$ and $\mathrm{Inv}_p\mathbf{K}_{(p)} = \mathrm{Inv}_\infty\mathbf{K}_{(p)} = \frac{1}{2}$.*

Finally, there exists at least one and upto isomorphisms, at most finitely many X in each characteristic for which (ii) *holds.*

PROOF. First consider the following three statements.

(A) X is of p-rank 0.

(B) End^0X is non-commutative.

(C) X is defined over a finite field, and if π is the Frobenius morphism over this field, $\pi^n = p_X^m$ for some n and $m > 0$.

We shall establish that (A) $\Longleftrightarrow$ (B) and (A) $\Longleftrightarrow$ (C) in that order.

Suppose then that (B) holds. A look at the table of §21 tells us that $\mathrm{End}^0(X)$ is a central simple quaternion algebra over $\mathbf{Q}$, hence $\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathrm{End}^0(X)$ is also a central simple algebra over $\mathbf{Q}_p$. If the p-rank of X were one, $\mathbf{Q}_p \otimes_{\mathbf{Z}_p} T_p(X)$ would be a one-dimensional $\mathbf{Q}_p$-vector space in which $\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathrm{End}^0X$ admits a representation, which is impossible. Hence X has p-rank 0, proving (A).

Next, suppose (A) holds and suppose End X were commutative, so that $\mathrm{End}^0X = K$ is an algebraic number field. Since every elliptic curve isogenous with X is again of p-rank zero, and there are only finitely many isomorphism classes of curves of p-rank 0, if R is the ring of integers of K, we can find an integer $N > 0$ such that for every X' isogenous to X, we have $N.R \subset \mathrm{End}\ X'$. Choose a prime l not dividing pN such that Rl is a prime ideal in R. (It is known that such l exist.) Let α be a non-zero element of $T_l(X)$ not divisible by l and let K_n be the cyclic subgroup generated by the image of α under the natural homomorphism $T_l(X) \to X_{l^n}$. Then $K_n \subsetneq K_{n+1}$. Again by the finiteness of the number of isomorphism classes of curves of p-rank 0, we can find integers $m > n$ such that $K_n \subsetneq K_m$ and there is an isomorphism $\xi: X/K_m \xrightarrow{\sim} X/K_n$. Thus, if $\eta: X/K_n \to X/K_m$ is the natural homomorphism induced by the inclusion $K_n \subset K_m$, we get an endomorphism $\alpha = \eta \circ \xi \in \mathrm{End}\ X'$, where $X' = X/K_m$, such that α has cyclic kernel of order l^k, $k > 0$. Since degree α and hence $\mathrm{Nm}_{K/\mathbf{Q}}\alpha$ is a power of l and Rl is a prime ideal in R, we must have $\alpha = l^r.u$ where u is a unit in R

and $r > 0$. So $N\alpha = l^r.Nu$, and $Nu \in \mathrm{End}\ X'$. Now, the degree of Nu is N^2 since u is a unit in R, so that the l-primary part of $\ker(l^r.Nu)$ is $(\mathbf{Z}/l^r\mathbf{Z})^2$. On the other hand, the l-primary part of $\ker(N\alpha)$ is isomorphic to $\ker\alpha$, which is cyclic. This contradiction proves (B).

We now prove that (A) $\Longleftrightarrow$ (C). We have already shown that (A) implies that X is defined over a finite field. Let π be the Frobenius morphism over this field. Since End X is finitely generated, we can find a finite extension of degree n, say, such that every element of End X is defined over this extension. Hence π^n commutes with End X, so π^n belongs to the center of End X. Since (A) holds, so does (B), so that End^0X is a quaternion algebra with center $\mathbf{Q}$. Hence, π^n is an integer, and by consideration of degree, $\pi^n = \pm p^m$ for some $m > 0$, so $\pi^{2n} = p^{2m}$. Conversely, if $\pi^n = p_X^m$ for some n and $m > 0$, then since π is bijective, p_X is also bijective and X has p-rank 0.

We have thus shown that (A) $\Longleftrightarrow$ (B) $\Longleftrightarrow$ (C). Next if End^0X is non-commutative, it is a quaternion division algebra over $\mathbf{Q}$, and since for $l \neq p$, $\mathbf{Q}_l \otimes_{\mathbf{Q}} \mathrm{End}^0X \to \mathrm{End}_{\mathbf{Q}_l}(\mathbf{Q}_l \otimes_{\mathbf{Z}_l} T_l(X))$ is injective and both sides have dimension 4 it is an isomorphism. Therefore $\mathrm{Inv}_l(\mathrm{End}^0X) = 0$ if l is finite and $l \neq p$. Since $\sum_v \mathrm{Inv}_v(\mathrm{End}^0X) = 0$, the sum being over the finite and infinite places of $\mathbf{Q}$, and $\mathrm{Inv}_\infty(\mathrm{End}^0X) = 0$ or $\frac{1}{2}$, we deduce that $\mathrm{Inv}_p(\mathrm{End}^0X) = \mathrm{Inv}_\infty(\mathrm{End}^0X) = \frac{1}{2}$. This establishes (b)(ii).

Next, we show that if X is defined over a finite field, $\mathrm{End}^0X \neq \mathbf{Q}$. We have proved this for X of p-rank 0. Suppose then that p-rank of X is 1. As before, π is an endomorphism of X which is bijective and of degree a power of p, so that it cannot equal m_X for any integer m. Thus, $\pi \in \mathrm{End}\ X$, $\pi \notin \mathbf{Z}$. It follows from the table of possibilities of §21 that then End^0X is an imaginary quadratic extension of $\mathbf{Q}$. This proves (b)(i).

We have also established therefore that if $\mathrm{End}^0X = \mathbf{Q}$, X cannot be defined over a finite field. Suppose finally that X is not defined over a finite field. We may assume X is the normal form

(N_p) in characteristic $p > 2$, with λ transcendental. (If $p = 2$, the argument still works if a somewhat different normal form is used.) Let us call this curve X_λ. Since any two transcendental elements λ and λ' over the prime field are conjugate over the prime field, we see that if $\mathrm{End}\, X_\lambda = A$, then $\mathrm{End}\, X_\mu \simeq A$ for any other transcendental μ over the prime field. Now, $\mathrm{End}^0 X$ must be either $\mathbf{Q}$ or an imaginary quadratic extension of $\mathbf{Q}$, since the only other possibility is that of a non-commutative division algebra, in which case, by the implication (B) $\Rightarrow$ (A) above, X_λ has p-rank 0 and λ must be algebraic. Suppose then that $\mathrm{End}^0 X$ is an imaginary quadratic extension of $\mathbf{Q}$. Then we can find an element α in A such that $\alpha^2 = N \in \mathbf{Z}$, $N < 0$. Hence for any transcendental μ over the prime field, there is an $\alpha_\mu \in \mathrm{End}\, X_\mu$ with $\alpha_\mu^2 = N$. Suppose l is a prime not dividing pN and $\xi \in T_l(X_\lambda)$. Let K_n be the cyclic group generated by the image of ξ under the map $T_l(X_\lambda) \to X_{l^n}$, and let $p: X_\lambda \to X_\lambda/K_n$ be the natural map. By our remarks preceding the theorem, X_λ/K_n is also not defined over a finite field, and is therefore of the form X_μ for some μ transcendental over the prime field. With α_μ as above, since the map $\mathrm{End}^0 X_\mu \to \mathrm{End}^0 X_\lambda$ given by $\alpha \longmapsto p^{-1} \circ \alpha \circ p$ is an isomorphism, we deduce that $(p^{-1} \circ \alpha_\mu \circ p)^2 = N_X$, and since $\alpha_\lambda^2 = N_X$ and $\mathrm{End}^0 X_\lambda$ is a commutative field, $p^{-1} \circ \alpha_\mu \circ p = \pm\, \alpha_\lambda$ and $\alpha_\mu \circ p = \pm\, p \circ \alpha_\lambda$. Thus, $\alpha_\lambda(\ker p) \subset \ker p$, that is, $\alpha_\lambda(K_n) \subset K_n$. Since this holds for every n, we deduce that $\alpha_\lambda(\xi) = a\xi$ for some $a \in \mathbf{Z}_l$. Thus, for α_λ acting as an endomorphism of $T_l(X_\lambda)$, every vector is an eigenvector, so that α_λ acts as a scalar on $T_l(X_\lambda)$. Since the characteristic polynomial of α_λ has integer coefficients, this scalar must be rational, and its square cannot be negative. This contradiction shows that if X is not defined over a finite field, $\mathrm{End}^0 X = \mathbf{Q}$, thereby proving (a).

A far-reaching generalization of part of this theorem to higher dimensions has been proven by Tate and Grothendieck. Suppose k has char p, and X is a simple abelian variety defined over k.

THEOREM. *X is isogenous to an X' defined over a finite field if and only if X is of CM-type.*

($\Rightarrow$ was proven by Tate : [T2]; $\Leftarrow$ was proven by Grothendieck: [G1]). Tate shows further :

THEOREM. *If X is defined over a finite field k_0, π is the Frobenius morphism over k_0, and $\mathrm{End}\,(X, k_0)$ is the ring of k_0-rational endomorphisms, then*

$$\mathrm{End}(X, k_0) \otimes \mathbf{Q}_l = \text{centralizer of } T_l(\pi) \text{ in } \mathrm{Hom}_{\mathbf{Q}_l}(T_l(X), T_l(X)).$$

23. **The group $\mathcal{G}(L)$.** There is a second approach to the Riemann form of a line bundle, via a technique which is important in other contexts such as the theory of moduli, and the closer study of linear systems on an abelian variety. We first make a group-theoretic digression to explain the class of group schemes that we will need.

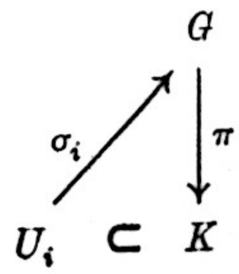
DEFINITION. *A theta-group will be a system of group schemes and homomorphisms*

$$1 \longrightarrow \mathbf{G}_m \xrightarrow{\ i\ } G \xrightarrow{\ \pi\ } K \longrightarrow 1$$

such that

(a) *K is commutative (but G need not be);*

(b) *$\exists$ an open covering $\{U_i\}$ of K and sections σ_i of π:*



(c) *i is a closed immersion, making $\mathbf{G}_m$ into the kernel of π;*

(d) *$\mathbf{G}_m \subset$ center of G.*

When K is a finite group scheme, there is a global section $\sigma: K \to G$ for π, and then *as a scheme*, $G \simeq \mathbf{G}_m \times K$ (i.e. define $\phi: \mathbf{G}_m \times K \to G$ by $\phi(\alpha, k) = i(\alpha).\sigma(k)$). Having made this splitting, the group law on G can be carried over to a "twisted" group law on $\mathbf{G}_m \times K$. There will be a morphism

$$f : K \times K \longrightarrow \mathbf{G}_m$$

such that the twisted group law is

$$(\alpha, k).(\alpha', k') = (\alpha.\,\alpha'.\,f(k, k'),\ k + k'), \qquad (*)$$

where α, α' are S-valued points of $\mathbf{G}_m$, k, k' are S-valued points of K, and K is written additively. f must be a 2-co-cycle :

$$f(k + k', k'').\, f(k, k') = f(k, k' + k'').\, f(k', k'')$$

and changing the section σ has the effect of altering f by a coboundary :

$$f^*(k, k') = f(k, k').\, g(k + k').\, g(k)^{-1}.\, g(k')^{-1}.$$

Conversely, given any such f, (*) makes $\mathbf{G}_m \times K$ into a theta-group. In other words, the set of all theta-groups over a fixed finite K is isomorphic to the cohomology group $H^2(K, \mathbf{G}_m)$, computed via morphism cochains.

The deviation of G from commutativity is easily measured by taking the commutator. For any two S-valued points x, y of G, (1) $xyx^{-1}y^{-1}$ is an S-valued point of $\mathbf{G}_m$ and (2) it depends only on $\pi(x)$, $\pi(y)$ and not on x, y. Therefore there is a morphism

$$e : K \times K \longrightarrow \mathbf{G}_m$$

such that

$$xyx^{-1}y^{-1} = e(\pi x,\ \pi y), \quad \text{all } x, y \in G(S), \text{ all } S.$$

It is easily checked that e is a skew-symmetric bihomomorphism :

(a) $e(k + k', k'') = e(k, k'').\, e(k', k'')$

(b) $e(k, k' + k'') = e(k, k').e(k, k'')$

(c) $e(k, k) = 1.$

If G admits a global section of K and so is described by a 2-co-cycle f, normalised by the condition $f(0, 0) = 1$, then

(d) $e(k, k') = f(k, k')/f(k', k).$

In case K is finite, the bi-homomorphism e also can be expressed asymmetrically as a homomorphism :

$$\gamma : K \longrightarrow \hat{K}.$$

In fact, if we regard $K \times K$ and $\mathbf{G}_m \times K$ as group-schemes over K via p_2 then (e, p_2): $K \times K \to \mathbf{G}_m \times K$ is a K-homomorphism, i.e. a K-valued character of K, or a morphism $\gamma : K \to \hat{K}$. If $\langle\ ,\ \rangle : K \times \hat{K} \to \mathbf{G}_m$ is the universal pairing, then in terms of S-valued points k, k' of K, γ is given by

$$e(k, k') = \langle k, \gamma(k') \rangle .$$

PROPOSITION. *If K is finite, $\gamma : K \to \hat{K}$ as above, then for every S-valued point x of G, $[\pi(x) \in \ker \gamma] \iff$ [x is in the center of G] i.e. for all schemes S' over S, and all S'-valued points y of G, $xy = yxy$.*

PROOF. In fact, $\gamma(\pi(x)) \neq 0 \iff$ the character $\gamma(\pi(x)) : K \times S \to \mathbf{G}_m \times S$ is non-trivial $\iff$ for some S'-valued point k of K, $\gamma(\pi(x))(k) \neq 1 \iff$ for some k, $\langle k, \gamma(\pi(x)) \rangle \neq 1 \iff$ for some k, $e(k, \pi(x)) \neq 1 \iff$ for some S'-valued point y of G, $xy \neq yx$.

COROLLARY. *The following are equivalent.*

(i) *γ is an isomorphism.*

(ii) *$i(\mathbf{G}_m)$ is exactly the center of G, i.e. every S-valued point x of G commuting with all S'-valued points, all S'/S, is in $i(\mathbf{G}_m)$.*

Such theta-groups will be called *non-degenerate.*

At the other extreme, we need two facts about when such G's are trivial.

LEMMA 1. (i) *If K is finite and G is commutative, then $G \simeq \mathbf{G}_m \times K$ as a group, i.e. in the category of commutative group schemes, K finite $\Rightarrow \mathrm{Ext}^1(K, \mathbf{G}_m) = (0)$.*

(ii) *If K is finite of prime order, then G is commutative.*

PROOF. (i) is a standard fact for commutative algebraic group schemes. For instance, once one sets up the long exact sequence for Ext's in this category, one takes a maximal chain of subgroups of K and reduces (i) to the special cases $K = \mathbf{Z}/l\mathbf{Z}$, $\mathbf{Z}/p\mathbf{Z}$, μ_p, or α_p. In the first two cases, one lifts a generator of K to a point of G of the same order (using the fact that k^* is divisible); in the second two cases, one checks by a direct computation that the

p-Lie algebra of G must split. For details, cf. Oort [O], or Séminaire Heidelberg-Strasbourg. To prove (ii), if $K = \mathbf{Z}/l\mathbf{Z}$ or $\mathbf{Z}/p\mathbf{Z}$, lift a generator of K to any point of G and note that if a reduced group scheme is generated by a central subgroup and one element, then it is commutative. If $K = \mu_p$ or α_p, let $\mathfrak{g}$ be the Lie algebra of G: then $\mathfrak{g} = k.x + k.y$ where x generates $\mathrm{Lie}\,\mathbf{G}_m$ and y lifts a generator of $\mathrm{Lie}\,K$. Since $\mathbf{G}_m$ is central in G, $[x, z] = 0$, all $z \in \mathfrak{g}$. Therefore $\mathfrak{g}$ is an abelian Lie algebra, which implies that $G^{(p)}$ is commutative (cf. Séminaire Heidelberg-Strasbourg or [G 3]. Since, as a scheme $G \simeq \mathbf{G}_m \times K$, any S-valued point of G is the product of S-valued points of $\mathbf{G}_m$ and of K, hence of S-valued points of $\mathbf{G}_m$ and of $G^{(p)}$. Since $\mathbf{G}_m$ is central and $G^{(p)}$ is commutative, this shows that G is commutative too.

The natural idea for proving (ii) would be to show that when K has prime order there are no non-trivial skew-symmetric bi-homomorphisms

$$e : K \times K \longrightarrow \mathbf{G}_m.$$

But this is false in char 2, if $K = \alpha_2$! This has fascinating consequences: cf. [Br].

We now return to abelian varieties. First of all, to eliminate any possible confusion, let me state clearly that if L is a line bundle over X, with projection $p : L \to X$, and $\sigma : X \to X$ is an automorphism of X, then by an automorphism $\tau : L \to L$ covering σ we always mean a *linear* automorphism fitting into a diagram :

$$\begin{array}{ccc} L & \xrightarrow{\tau} & L \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle p} \\ X & \xrightarrow[\sigma]{} & X. \end{array}$$

Moreover, such a τ induces an isomorphism $\tau' : L \xrightarrow{\sim} \sigma^* L$ and any such isomorphism τ' induces an automorphism τ of L covering σ.

Secondly, recall that if X is an abelian variety, S any scheme and $f : S \to X$ is an S-valued point of X, then T_f, translation by f, denotes the S-isomorphism of schemes $(p_1, m \circ (f \times 1_X)) : S \times X \to S \times X$, where m is the multiplication on X.

Now here is how theta groups arise.

THEOREM 1. *Let L be a line bundle on an abelian variety X. For any scheme S, let* $\underline{\mathrm{Aut}}\,(L/X)(S)$ *be the group of automorphisms of $S \times L$ covering a translation map of $S \times X$.* $\underline{\mathrm{Aut}}\,(L/X)$ *is a contravariant group-valued functor on* $\underline{\mathrm{Sch}}$. *Then there is a group scheme $\mathcal{G}(L)$ and an isomorphism of group functors*

$$\underline{\mathrm{Aut}}(L/X) \simeq \mathcal{G}(L).$$

For any scheme S, the natural homomorphisms of groups

$$1 \to H^0(S, \mathcal{O}_S^*) \to \underline{\mathrm{Aut}}\,(L/X)(S) \to \left\{ \begin{array}{l} S\text{-valued points } f : S \to X \\ \text{such that} \\ T_f^*(S \times L) \simeq S \times L \end{array} \right\} \to 1$$

induce homomorphisms of group schemes

$$1 \longrightarrow \mathbf{G}_m \xrightarrow{i} \mathcal{G}(L) \xrightarrow{j} K(L) \longrightarrow 1$$

making $\mathcal{G}(L)$ into a theta-group.

PROOF. Let L^* be the complement of the 0-section in L; this is a principal fibre bundle over X with structure group $\mathbf{G}_m$. Fix a base point $P_0 \in p^{-1}(0) \cap L^*$, and put $\mathcal{G}(L) = p^{-1}(K(L)) \cap L^*$. For any automorphism α of $S \times L$ covering a translation T_f of $S \times X$, where $f \in X(S)$, we get a morphism $\tilde{\alpha} : S \to L^*$ defined by $\tilde{\alpha} = p_2 \circ \alpha \circ s_0$, where s_0 is the map $S \simeq S \times \{P_0\} \hookrightarrow S \times L$ and $p_2 : S \times L \to L$ is the projection. Since $p \circ \tilde{\alpha}$ is just the morphism f, and $f \in K(L)\,(S)$, we deduce that $\tilde{\alpha}$ factors through $\mathcal{G}(L)$:

$$S \xrightarrow{\bar{\alpha}} \mathcal{G}(L) \hookrightarrow L^*.$$

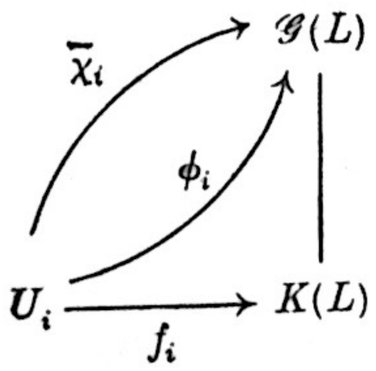
Then $\alpha \longmapsto \alpha$ defines a map

$$\underline{\mathrm{Aut}}\,(L/X)(S) \to \mathcal{G}(L)(S),$$

which is functorial in S. I claim that it is an isomorphism. Suppose $\alpha, \beta \in \underline{\mathrm{Aut}}\ (L/X)(S)$ covering T_f and T_g respectively, are such that $\bar{\alpha} = \bar{\beta}$. We then have $f = p \circ \bar{\alpha} = p \circ \bar{\beta} = g$, and $\gamma = \beta \circ \alpha^{-1}$ is an automorphism of $S \times L$ over the base $S \times X$ such that the composite $S \xrightarrow{s_0} S \times L \xrightarrow{\gamma} S \times L$ equals s_0. Now, γ is given by multiplication by an element γ_1 of $H^0(S \times X, \mathcal{O}^*_{S \times X})$ and since $s_0 = \gamma \circ s_0$, $\gamma_1 | S \times \{P_0\} = 1$. But $H^0(S \times X, \mathcal{O}^*_{S \times X}) \simeq H^0(S, \mathcal{O}^*_S)$, so $\gamma_1 = 1$ and $\gamma = 1_{S \times L}$. This proves that the map $\alpha \longmapsto \bar{\alpha}$ is injective. To prove that it is surjective, let $\phi \in \mathcal{G}(L)(S)$, and let $f = p \circ \phi$ so that $f \in K(L)(S)$. Then by definition of $K(L)$,

$$T_f^*(S \times L) \simeq (S \times L) \otimes p_1^* M$$

for some line bundle M on S. We can cover S by open sets $\{U_i\}$ such that $M|_{U_i}$ is trivial. Then over $U_i \times X$, $T_f^*(S \times L)$ and $S \times L$ are isomorphic, so there exist automorphisms χ_i of $U_i \times L$ covering T_{f_i}, f_i = restriction of f to U_i. If ϕ_i is the restriction of ϕ to U_i, we now have two liftings of the morphism f_i to $\mathcal{G}(L)$:



Since $\mathcal{G}(L)$ is a principal fibre bundle over $K(L)$ with group $\mathbf{G}_m$, there is a unit $\epsilon_i \in \Gamma(U_i, \mathcal{O}^*_S)$ such that $\phi_i = \epsilon_i(\bar{\chi}_i)$. But if λ_i is the automorphism, mult. by ϵ_i, of $U_i \times L$, then $\overline{\lambda_i \chi_i} = \epsilon_i(\bar{\chi}_i) = \phi_i$. Finally, since ϕ_i agrees with ϕ_j on $U_i \cap U_j$, the two automorphisms $\lambda_i \chi_i$ and $\lambda_j \chi_j$ agree on $(U_i \cap U_j) \times L$ (using injectivity of $\alpha \longmapsto \bar{\alpha}$), so there is an automorphism χ of $S \times L$ extending $\lambda_i \chi_i$. Then $\bar{\chi} = \phi$ so $\alpha \longmapsto \bar{\alpha}$ is a surjective map.

This establishes an isomorphism of functors $\underline{\mathrm{Aut}}\ (L/X) \simeq \underline{\mathcal{G}(L)}$, and since the left side is a group functor, $\mathcal{G}(L)$ becomes a

group scheme. Define homomorphisms $i: \mathbf{G}_m \to \mathcal{G}(L)$ and $j: \mathcal{G}(L) \to K(L)$ by the homomorphisms of functors:

$$\mathbf{G}_m(S) = \Gamma(S, \mathcal{O}^*_S) \longrightarrow \underline{\mathrm{Aut}}(L/X)(S) \simeq \mathcal{G}(L)(S)$$
$$\epsilon \longmapsto \text{mult. by } \epsilon$$

$$\mathcal{G}(L)(S) \simeq \underline{\mathrm{Aut}}\ (L/X)(S) \longrightarrow K(L)(S)$$
$$\alpha \longmapsto \left\{ \begin{array}{l} \text{the } S\text{-valued point } f \text{ of } X \\ \text{such that } \alpha \text{ covers } T_f \end{array} \right\}.$$

Then i is clearly injective, j is just the projection p, and $\mathrm{Im}(i) = \mathrm{Ker}(j)$. Since there are sections locally to p: $L \to X$, there are also sections locally to $j: \mathcal{G}(L) \to K(L)$. Finally, if $\epsilon \in \Gamma(S, \mathcal{O}^*_S)$, then the automorphism, mult. by ϵ, clearly commutes with all other automorphisms $\alpha \in \underline{\mathrm{Aut}}\ (L/X)(S)$, so $i(\mathbf{G}_m)$ is in the center of $\mathcal{G}(L)$. This proves that $\mathcal{G}(L)$ with i and j is a theta-group.

DEFINITION. *$e^L: K(L) \times K(L) \to \mathbf{G}_m$ is the skew-symmetric bihomomorphism associated to the commutator in the theta-group $\mathcal{G}(L)$.*

Look at the case $L \in \mathrm{Pic}^0 X$. Then $K(L) = X$ and the morphism e^L takes the complete variety $X \times X$ to the affine variety $\mathbf{G}_m$. Therefore $e^L \equiv 1$ and $\mathcal{G}(L)$ is a commutative group scheme, which is an extension of X by $\mathbf{G}_m$. It can in fact be shown that this map:

$$\mathrm{Pic}^0(X) \longrightarrow \underset{\substack{\text{comm.group} \\ \text{schemes}}}{\mathrm{Ext}^1}(X, \mathbf{G}_m)$$
$$L \longmapsto \mathcal{G}(L)$$

is an isomorphism (Theorem of Serre and Rosenlicht).

Suppose next that the line bundle L arises from a divisor D: $L \simeq \mathcal{O}_K(D)$. We leave it to the reader to check that the discrete group $\mathcal{G}(L)_k$ can be described as follows.

$$\mathcal{G}(L)_k = \{(x, f) \mid x \in X, f \in k(X), T_x^{-1} D = D + (f)\}$$

$$(x, f) \cdot (y, g) = (x + y, T_x^* g \cdot f).$$

This works since

$$T_{x+y}^{-1}D - D - (T_x^* g + f) = T_x^{-1}(T_y^{-1}D - D) + (T_x^{-1}D - D) - T_x^{-1}(g) - (f)$$
$$= T_x^{-1}(T_y^{-1}D - D - (g)) + (T_x^{-1}D - D - (f)) = 0.$$

The subgroup $k^* = (\mathbf{G}_m)_k \subset \mathscr{G}(L)_k$ corresponds to the pairs $x = 0$, $f = \alpha \in k^*$; the projection $\mathscr{G}(L)_k \to K(L)_k$ corresponds to the map $(x, f) \longmapsto x$.

FUNCTORIAL PROPERTIES OF e^L.

In the following formulas, the symbols x, y etc. are to be understood as R-valued points for any k-algebra R. One could equivalently interpret the formulas as commutativity of certain diagrams of morphisms. With this specific understanding, we shall often omit R from the statements and proofs and speak as though we were just dealing with ordinary points, but all the assertions are to be understood in the stronger sense mentioned.

(1) If $f: X \to Y$ is a homomorphism of abelian varieties and L a line bundle on Y, we have

$$e^{f^*(L)}(x, y) = e^L(f(x), f(y)),\ x, y \in f^{-1}(K(L)).$$

(2) For any line bundles L_1, L_2 on X,

$$e^{L_1 \otimes L_2}(x, y) = e^{L_1}(x, y) \cdot e^{L_2}(x, y),\ x, y \in K(L_1) \cap K(L_2).$$

(3) For algebraically equivalent line bundles L_1, L_2 on X, $e^{L_1} = e^{L_2}$.

(4) For $x \in K(L)$ and $y \in n_X^{-1}(K(L))$,

$$e^{L^n}(x, y) = e^L(x, ny).$$

(5) For $x \in X_n$, $y \in n_X^{-1}(K(L)) = \phi_L^{-1}(X_n)$, ($n$ any integer with $p \nmid n$)

$$\bar{e}_n(x, \phi_L(y)) = e^{L^n}(x, y).$$

PROOFS. (1) We may assume $f(x) = j(\xi)$, $f(y) = j(\eta)$, where $j: \mathscr{G}(L) \to K(L)$ is the natural homomorphism. (When x, y are R-valued points, we can find ξ, η after localizing on Spec R.) We

can then lift ξ and η to automorphisms ϕ, ψ of $f^*(L)$ covering T_x and T_y respectively, and then $\phi\psi\phi^{-1}\psi^{-1}$ lifts $\xi\eta\xi^{-1}\eta^{-1}$, which means precisely (1).

(2) Again we may assume that there are automorphisms ϕ_i, ψ_i respectively of L_i, $i = 1, 2$, covering T_x and T_y. Then $\phi_1 \otimes \phi_2$ and $\psi_1 \otimes \psi_2$ are automorphisms of $L_1 \otimes L_2$ covering T_x, T_y respectively, and the commutator of these two automorphisms is the tensor product of the commutators of ϕ_i and ψ_i ($i = 1, 2$), which proves (2).

(3) Write $L_3 = L_1 \otimes L_2^{-1}$, so that $L_3 \in \mathrm{Pic}^0 X$ and $L_1 = L_2 \otimes L_3$, $K(L_3) = X$. Apply (2) to the line bundles L_2 and L_3.

(4) By replacing the ring R by a ring $R' \supset R$ if necessary, we may assume $x = nz$ for some $z \in n_X^{-1}(K(L))$. (In fact, we have only to take Spec R' = Spec $R \times_{K(L)} n_X^{-1}(K(L))$ which is finite and flat over Spec R, so that it is affine and $R' \supset R$.) We then have $z, y \in n_X^{-1}(K(L)) = K(L^n)$, so that by (1) applied to $n_X^*(L)$ and (2) applied repeatedly, and making use of the algebraic equivalence of $n_X^*(L)$ and L^{n^2}, we obtain

$$e^L(nz, ny) = e^{n_X^*(L)}(z, y)$$
$$= e^{L^{n^2}}(z, y)$$
$$= (e^{L^n}(z, y))^n$$
$$= e^{L^n}(nz, y),$$

which is formula (4).

(5) As in (4), we may assume that $y = nz$ for some z, and the equation to be proved assumes the form

$$\bar{e}_n(x, \phi_L(y)) \stackrel{?}{=} e^{L^n}(x, nz) = e^{L^{n^2}}(x, z) = e^{n_X^*(L)}(x, z)$$

since L^{n^2} is algebraically equivalent to $n_X^*(L)$ and $z \in K(L^{n^2}) = K(n_X^*(L))$. The fact that $z \in K(n_x^*(L))$ means that we have an automorphism σ of $n_X^*(L)$ covering the translation T_z (localize Spec R if need be).

Let us agree to denote (temporarily), for line bundles M, N on X, the line bundle associated to the locally free sheaf of germs of homomorphisms of M into N by $\mathrm{Hom}(M, N)$, so that we have a natural isomorphism $\mathrm{Hom}(M, N) \xleftarrow{\sim} M^{-1}\otimes N$. Note that there is a natural action of X_n on any pull back $n_X^*(M)$ covering translations, hence also natural actions on tensor products, Homs and translates of pull-backs (this last, since any translation commutes with any other). With this understanding, we have *natural* isomorphisms of the following line bundles on X commuting with this X_n action:

$$n_X^*(T_y^*L\otimes L^{-1}) \approx n_X^*(T_y^*(L))\otimes n_X^*(L^{-1}) \approx T_z^*(n_X^*(L))\otimes n_X^*(L)^{-1}$$
$$\approx \mathrm{Hom}\,[n_X^*(L), T_z^*(n_X^*(L))].$$

But what is $\bar{e}_n(\cdot, \phi_L(y))$? $n_X^*(T_y^*L\otimes L^{-1})$ is isomorphic to the trivial bundle, and $\bar{e}_n(\cdot, \phi_L(y))$ is given in the usual way by the natural action of X_n carried over to the trivial bundle. Equivalently, $n_X^*(T_y^*L\otimes L^{-1})$ has a nowhere vanishing section, unique up to scalars, and $e_n(\cdot, \phi_L(y))$ is given by the action on X_n on this section. Now make this computation on the bundle on the right instead of the one on the left. A nowhere vanishing section of the line bundle on the right is just an isomorphism $n_X^*(L) \xrightarrow{\phi} n_X^*(L)$ covering T_z, and the natural action of $x \in X_n$ on the right maps this section into the section ϕ': $n_X^*(L) \to n_X^*(L)$ defined by $\phi' = \eta_x \circ \phi \circ \eta_x^{-1}$, where η_x: $n_X^*(L) \to n_X^*(L)$ is the natural isomorphism covering T_x. We must therefore have $\eta_x \circ \phi \circ \eta_x^{-1} = e_n(x, \phi_L(y)).\phi$. Applying this in particular to the automorphism σ covering T_z chosen earlier, we get that $\eta_x \circ \sigma \circ \eta_x^{-1} \circ \sigma^{-1} = \bar{e}_n(x, \phi_L(y))$. But this means by definition that $e^{n_X^*(L)}(x, z) = e_n(x, \phi_L(y))$.

As a corollary, we get a second proof of the skew-symmetry of the Riemann form of L:

$$\bar{e}_n(x, \phi_L(y)) = e^{L^n}(x, y) = e^{L^n}(y, x)^{-1} = e_n(y, \phi_L(x))^{-1},$$

if $x, y \in X_n$. The formula (5), coupled with (4), shows how the Riemann forms can be computed from the e^L's and conversely, how all the e^L's, on points of order l^n, can be computed from the Riemann forms.

THEOREM 2. *Suppose $\pi: X \to Y$ is an isogeny of abelian varieties, and L is a line bundle on X. Then there is a natural one-one correspondence between*

(a) *isomorphism classes of line bundles M on Y such that $\pi^*M \simeq L$,*

(b) *homomorphisms $\alpha: \ker \pi \to \mathcal{G}(L)$ lifting the inclusion* $\ker \pi \hookrightarrow X$.

PROOF. This is just a restatement, in a special case of the general descent theorem in §12 for coherent sheaves with respect to quotients by finite group schemes. Use the fact that

$$\mathrm{Hom}_X(\ker \pi, \mathcal{G}(L)) \simeq \left\{\begin{array}{l}\text{actions of } \ker \pi \text{ on } L \text{ covering}\\ \text{its translation action on } X\end{array}\right\}.$$

COROLLARY. *Given $\pi: X \to Y$ and L as above. Then a line bundle M on Y such that $\pi^*M \simeq L$ exists if and only if* $\ker(\pi) \subset K(L)$ *and* $e^L|_{\ker \pi \times \ker \pi} \equiv 1$.

PROOF. Let $p: \mathcal{G}(L) \to K(L)$ be the projection and let $G = p^{-1}(\ker \pi)$. Then G is a theta-group over $\ker \pi$, and by part (i) of the lemma at the beginning of this §, $e^L|_{\ker \pi \times \ker \pi} \equiv 1 \iff G$ is commutative $\iff G \simeq \mathbf{G}_m \times \ker \pi$ as group-scheme $\iff \exists$ a homomorphism $\alpha: \ker \pi \to G$ such that $p\circ\alpha = 1 \iff M$ exists.

We now prove the following theorem, promised in §20.

THEOREM 3. *If L is a line bundle on an abelian variety X and $n \in \mathbf{Z}$, $L \simeq M^n$ for some line bundle M if and only if $K(L) \supset X_n$.*

PROOF. The 'only if' part follows from the equation $\phi_L = n\phi_M$. Assume conversely that $K(L) \supset X_n$. To show that $L \simeq M^n$ for some line bundle M, it suffices to show that $L^n \simeq n_X^*(N)$ for some N. Indeed, we would then have that $(L\otimes N^{-n})^n \in \mathrm{Pic}^0X$, hence also $L\otimes N^{-n} \in \mathrm{Pic}^0X$, and if we choose $P \in \mathrm{Pic}^0X$ such that $L\otimes N^{-n} \simeq P^n$, we would obtain $L \simeq (N\otimes P)^n$.

To show that $L^n \simeq n_X^*(N)$, we merely compute, for any R-valued points x, y of X_n,

$$e^{L^n}(x,y) = e^L(x,ny) = 1.$$

The desired conclusion then follows from the corollary to Theorem 2.

Our last result concerns the non-degeneracy of $\mathcal{G}(L)$. We need some preliminary results.

Suppose $e\colon K \times K \to \mathbf{G}_m$ is a skew-symmetric bi-homomorphism on a finite group K. Let $\gamma\colon K \to \hat{K}$ be the associated homomorphism. Then if $H \subset K$ is a subgroup, I claim that there is a second subgroup $H^\perp$ characterized by the property:

$$\text{if } k \text{ is an } S\text{-valued point of } K,$$

$$k \in H^\perp(S) \iff \{\text{for all } S'/S, \text{ all } S'\text{-valued points } k' \text{ of } H,\ e(k,k') = 1\}.$$

In fact, restricting characters of K to H defines a morphism $q\colon \hat{K} \to \hat{H}$, and $H^\perp$ is clearly the kernel of $q \circ \gamma\colon K \to \hat{H}$. Now suppose $\pi\colon X \to Y$ is an isogeny of abelian varieties, M is a line bundle on Y and $L = \pi^*M$. Let $H = \ker(\pi)$: then as we have seen H is a subgroup of $K(L)$ such that $e^L|_{H\times H} \equiv 1$. In other words, $H \subset H^\perp$. The result we require is

LEMMA 2. $K(M) \simeq H^\perp/H$.

PROOF. Let $x\colon S \to X$ be an S-valued point of X. We must show that x is a point of $H^\perp$ if and only if πx is a point of $K(M)$. It will suffice to prove this when $S = \mathrm{Spec}(R)$, R a local ring, in which case S carries only trivial line bundles. Then, using the descent theorem of §12,

$$\pi x \in K(M)(S) \iff T_{\pi x}^*(S \times M) \simeq S \times M$$

$$\iff \left\{ \begin{array}{l} \exists \text{ an isomorphism } T_x^*(S \times L) \simeq S \times L \\ \text{commuting with the action of } \ker \pi \text{ on} \\ \text{these two line bundles} \end{array} \right\}.$$

Now suppose $\alpha : H \to \mathcal{G}(L)$ is the homomorphism giving the action of H on L for which M is the quotient. Then we continue our equivalences:

$$\iff \left\{ \begin{array}{l} \exists \text{ an } S\text{-valued point } w \text{ of } \mathcal{G}(L) \text{ such that} \\ p(w) = x \text{ and } w \text{ commutes with } \alpha(H) \end{array} \right\}$$

$$\iff \{e^L(x, h) = 1, \text{ all } S'\text{-valued points } h \text{ of } H\}$$

$$\iff x \in H^\perp(S).$$

The same argument shows in fact that

$$\mathcal{G}(M) \simeq \left\{ \begin{array}{c} \text{centralizer of } \alpha(H) \\ \text{in } \mathcal{G}(L) \end{array} \right\} \Big/ \alpha(H)$$

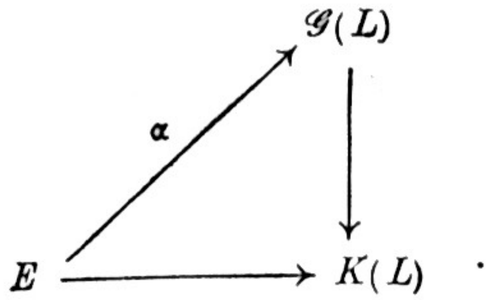
but we do not need this fact. We now apply the lemma to

THEOREM 4. *Let L be a non-degenerate line bundle on an abelian variety X. If $H \subset K(L)$ is a maximal subgroup such that $e^L|_{H\times H} \equiv 1$, then $H = H^\perp$ and* order $(H)^2 =$ order $(K(L))$.

PROOF. Let H be a maximal subgroup scheme of $K(L)$ such that $e^L|_{H\times H} \equiv 1$. Let $Y = X/H$, and let $\pi\colon X \to Y$ be the natural homomorphism. By the Cor. to Th. 2 there exists a line bundle M on Y such that $\pi^*M \simeq L$. The fact that H is maximal means that there are no further isogenies $\pi'\colon Y \to Y'$ for which $M \simeq \pi'^*(M')$ except the identity.

LEMMA 3. *Let L be a non-degenerate line bundle on an abelian variety X. If there are no isogenies $\pi\colon X \to Y$ of degree > 1 such that $L \simeq \pi^*M$, some line bundle M on Y, then $|\chi(L)| = 1$.*

PROOF. If $|\chi(L)| > 1$, then $K(L)$ is non-trivial. Then there exists a subgroup $E \subset K(L)$ of prime order, i.e., $E \simeq \mathbf{Z}/l\mathbf{Z}$, $\mathbf{Z}/p\mathbf{Z}$, μ_p or α_p. Look at the inverse image E in $\mathcal{G}(L)$: this is a theta-group scheme G over E. By the lemma at the beginning of this section, G is commutative, hence $G \simeq \mathbf{G}_m \times E$, hence there exists a homomorphism:



Therefore by Theorem 2, L descends to X/E, contradicting the assumption. So $|\chi(L)| = 1$.

Returning to the proof of the theorem, we deduce that $K(M) = (0)$ and $|\chi(M)| = 1$. Therefore by Lemma 2, $H = H^{\perp}$, and by the results of §16,

$$|\chi(L)| = \deg(\pi) = \text{order } (H),$$
$$\chi(L)^2 = \deg(\phi_L) = \text{order } (K(L));$$

so order $(H)^2 =$ order $K(L)$.

COROLLARY 1. *Every abelian variety X is isogenous to a principally polarized abelian variety Y, i.e. one which carries an ample line bundle L with $\chi(L) = 1$.*

PROOF. Apply the theorem to any ample L on X, and let $Y = X/H$, H maximal in $K(L)$ with $e^L|_{H\times H} \equiv 1$. Then $L \simeq \pi^*(M)$ and M is ample with $\chi(M) = 1$.

COROLLARY 2. *If L is a non-degenerate line bundle on X, then $\mathscr{G}(L)$ is a non-degenerate theta-group.*

PROOF. Let $\gamma\colon K(L) \to \hat{K}(L)$ be the homomorphism associated to e^L and suppose D is its kernel. Choose an $H \subset K(L)$ with $H = H^{\perp}$ and order $(H)^2 =$ order $K(L)$, as in the theorem. Now since $\gamma(D) = (0)$, we find

$$e^L|_{D\times K(L)} \equiv 1 \text{ and } e^L|_{K(L)\times D} \equiv 1.$$

Therefore $D \subset H^{\perp}$, so $D \subset H$ and also all characters $e(x)$ annihilate D, all $x \in K(L)(S)$. Now by definition, $H^{\perp}$ is the kernel of the homomorphism $K(L) \xrightarrow{\gamma} \hat{K}(L) \xrightarrow{q} \hat{H}$. It follows that $\text{Im}(q\circ\gamma) \subset (\hat{H}/D)$ and that we have an exact sequence

$$0 \longrightarrow H \longrightarrow K(L) \xrightarrow{q\circ\gamma} \hat{H}/D.$$

Therefore

$$\text{order } K(L) \leqslant \text{order } H.\ \text{order } \hat{H}/D$$
$$= (\text{order } H)^2/\text{order } D.$$

This proves that order $D = 1$.

The next step in the development of the theory of theta-groups is to show that (1) all representations of non-degenerate theta-groups which restrict to the identity character on the center G_m are completely reducible, (2) that there is only one irreducible representation with this property, and (3) that when L is non-degenerate, $i = i(L)$, then $\mathscr{G}(L)$ acts naturally on $H^i(X, L)$ and that this is the irreducible representation in (2). For these facts and their application, cf. [M2].

24. **The case $k = \mathbf{C}$.** The purpose of this last section is to tie together the algebraic approach of this chapter with the analytic methods of Chapter I. In particular, I want to relate the analytic and algebraic Riemann forms of a line bundle L, and I want to show how the positivity of the Rosati involution follows immediately from the positivity of the analytic Riemann form in its guise as a Hermitian form when L is ample.

As always, let $X = V/U$, V a complex vector space and U a lattice. Let $L = L(H,\alpha)$ be a line bundle on X, where H is a Hermitian form on V such that $E = \text{Im } H$ is integral on U, and $\alpha\colon U \to \mathbf{C}_1^*$ is a function such that

$$\alpha(u_1 + u_2) = \alpha(u_1).\alpha(u_2).e^{\pi i E(u_1,u_2)}.$$

Consider the group $\tilde{\mathscr{G}}$ of analytic automorphisms $\psi_{\sigma,u}$ of $\mathbf{C}\times V$ given by

$$\psi_{\sigma,w}(\lambda, z) = (\lambda.\sigma.e^{\pi H(z,w)},\ z + w)$$
$$\sigma \in \mathbf{C}^*,\ w \in V.$$

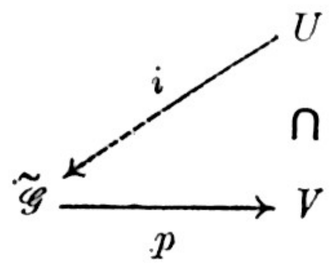
Then

$$\psi_{\sigma,w} \circ \psi_{\tau,v} = \psi_{\rho,w+v}$$
$$\rho = \sigma.\ \tau.\ e^{\pi H(v,w)},$$

so $\widetilde{\mathcal{G}}$ is an extension analogous to the theta-groups of §23:

$$1 \longrightarrow \mathbf{C}^* \xrightarrow{j} \widetilde{\mathcal{G}} \xrightarrow{p} V \longrightarrow 1$$
$$\psi_{\sigma,w} \xmapsto{p} w$$
$$\sigma \xmapsto{j} \psi_{\sigma,0}.$$

The data α defines a lifting i of U into $\widetilde{\mathcal{G}}$:

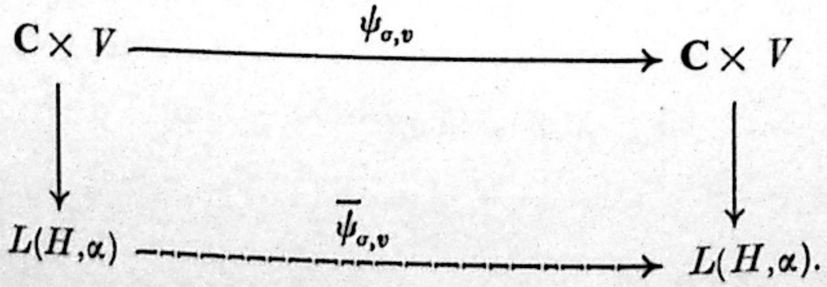


$$i(u) = \psi_{\sigma,u},\ \sigma = \alpha(u) \cdot e^{\frac{\pi}{2} H(u,u)},$$

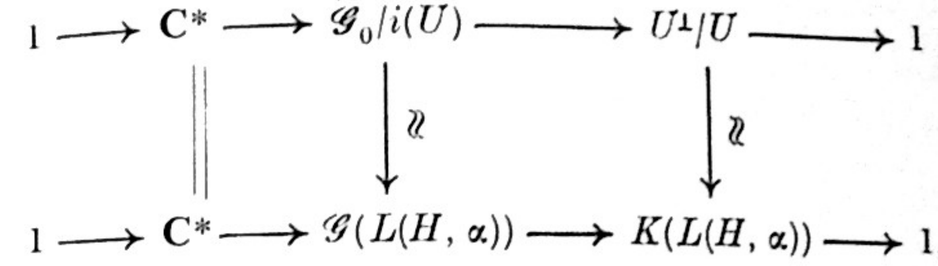
so that $L(H,\alpha)$ is, by definition, the quotient $\mathbf{C} \times V/i(U)$. The commutator in $\widetilde{\mathcal{G}}$, as in the theta-groups of §23, is given by a bi-homomorphism $\widetilde{e}: V \times V \to \mathbf{C}_1^*$ as follows:

$$\psi_{\sigma,w} \circ \psi_{\tau,v} \circ \psi_{\sigma,w}^{-1} \circ \psi_{\tau,v}^{-1} = \psi_{\widetilde{e}(v,w),0},$$
$$\widetilde{e}(v,w) = e^{2\pi i E(v,w)}.$$

Therefore, if $U^\perp = \{u \in V \mid E(u,u') \in \mathbf{Z},\ \text{all } u' \in U\}$ as before, it follows that the group $\widetilde{\mathcal{G}}_0 \underset{\text{def}}{=} p^{-1}(U^\perp) = \{\psi_{\sigma,v} \mid v \in U^\perp\}$ is the centralizer of $i(U)$ in $\widetilde{\mathcal{G}}$. Therefore, all the automorphisms $\psi_{\sigma,v}$, $v \in U^\perp$, descend to automorphisms $\bar{\psi}_{\sigma,v}$ of $L(H,\alpha)$:



This gives us a natural homomorphism $\mathcal{G}_0 \to \mathcal{G}(L(H,\alpha))$. But we saw in §9 that $K(L(H,\alpha)) \simeq U^\perp/U$, so we get in fact isomorphic extensions:



It follows that the commutators in these two groups are equal, hence we have proven

THEOREM 1. *If $L = L(H,\alpha)$ is a line bundle on $X = V/U$, $E = \operatorname{Im} H$, and $\pi : V \to X$ is the natural map, then for all $x, y \in U^\perp$:*

$$e^{-2\pi i E(x,y)} = e^L(\pi x, \pi y).$$

Since our ground field is $\mathbf{C}$, there is a canonical primitive n^{th} root of 1 for all n, namely $\zeta_n = e^{2\pi i/n}$. Therefore the module

$$M_l = \lim_{\leftarrow} \mu_{l^n}$$

has a canonical basis element ζ too, given by the sequence $e^{2\pi i/l^n} \in \mu_{l^n}$. We can now relate the Riemann forms

$$E: U \times U \to \mathbf{Z}, \text{ where } E = \operatorname{Im} H,$$
$$E^L: T_l X \times T_l X \to M_l, \text{ defined in § 20.}$$

Let π_l denote the natural map from U to $T_l X$, i.e. $\pi_l(u)$ is given by the sequence $u_n = \pi(u/l^n) \in X_{l^n}$, with $l u_{n+1} = u_n$. Then if $u, v \in U$,

$$E^L(\pi_l u, \pi_l v) = \text{the sequence } \bar{e}_{l^n}(u_n, \phi_L v_n)$$
$$= \text{the sequence } e^{L l^n}(u_n, v_n) \text{ (§ 23, property (5))}$$
$$= \text{the sequence } e^{-2\pi i l^n E(u/l^n,\, v/l^n)} \quad \text{(Theorem 1)}$$
$$= \text{the sequence } (\zeta_n)^{-E(u,v)}$$
$$= -E(u, v).\zeta.$$

Thus, except for sign, E^L is the $\mathbf{Z}_l$-linear extension of E from U to $T_l X$.

Applying this to the case where X is $Y \times \hat{Y}$ and L is the Poincaré bundle P, we see that the canonical non-degenerate integral pairing of the lattices U and $\hat{U}$ corresponding to Y and $\hat{Y}$, of the analytic theory (cf. §9, part (B)) is, up to sign, the same as the canonical non-degenerate l-adic pairing e_l of $T_l Y$ and $T_l \hat{Y}$ (cf. §20).

Next, consider the Rosati involution of $\mathrm{End}^0(X)$. Analytically, we use the interpretation:

$$\mathrm{End}^0(X) = \left\{ \begin{array}{l} \text{set of complex-linear endomorphisms } T\colon V \to V \\ \text{such that } T(\mathbf{Q}.U) \subset \mathbf{Q}.U \end{array} \right\}.$$

Then the natural involution is the adjoint with respect to H:

$$H(T^*x, y) = H(x, Ty), \quad \text{all } x, y \in V.$$

Since if $x \in \mathbf{Q}.U$, then for all $y \in \mathbf{Q}.U$, $E(T^*x, y) = E(x, Ty) \in \mathbf{Q}$, it follows that T^*x must be in $\mathbf{Q}.U$ too, i.e. $T^* \in \mathrm{End}^0(X)$. If T' is the image of T under the algebraic Rosati involution, then for all $x, y \in U$,

$$\begin{aligned} E((T^* - T')x, y) &= \mathrm{Im}\, H(T^*x, y) + E^L(T'\pi_l x, \pi_l y) \\ &= \mathrm{Im}\, H(x, Ty) + E^L(\pi_l x, T\pi_l y) \\ &= E(x, Ty) - E(x, Ty) = 0\ . \end{aligned}$$

Thus $T^* = T'$.

Now for any complex-linear operator $T\colon V \to V$, if T^* is its adjoint, then T^*T is a positive self-adjoint operator on the Hermitian vector space V, hence all its eigenvalues are positive, hence the complex trace, $\mathrm{Tr}(T^*T)$, is positive. If $T \in \mathrm{End}^0(X)$, so that T^*T maps the rational vector space $\mathbf{Q}.U$ into itself, its trace here is just twice its complex trace; and its l-adic trace in $T_l X \cong U \otimes \mathbf{Z}_l$ is equal to its rational trace. Therefore for any of these traces,

$$\mathrm{Tr}(T^* \circ T) > 0, \text{ all } T \in \mathrm{End}^0(X),\ T \neq 0.$$

Thus the positivity of the Rosati involution is obvious from the existence of the positive definite H with $\mathrm{Im}\, H = E$. In a sense, we have shown that over any ground field one can reverse this argument: namely, using the positivity of the Rosati involution, we have realised $NS^0(X)$ as a formally real Jordan algebra in which the ample L's are the positive elements.

BIBLIOGRAPHY

[A-G] A. Andreotti and H. Grauert : Théorèmes de finitude pour la cohomologie des espaces complexes, *Bull. Soc. Math. France*, 90 (1962), 193.

[B] Walter Baily : On the theory of θ-functions, the moduli of abelian varieties, and the moduli of curves, *Annals of Math.* 75 (1962), 342.

[B-K] H. Braun and M. Koecher : *Jordan Algebren*, Springer-Verlag, 1966.

[B-M] Armand Borel and George Mostow : editors, *Algebraic groups and discontinuous subgroups*, American Math. Soc. Providence, 1966.

[Br] L. Breen : On a non-trivial higher extension of representable abelian sheaves, *Bull. American Math. Soc.* 75 (1969), 1249.

[Bt] Iacopo Barsotti : Metodi analitici per varietà abeliane in caratteristica positiva, *Annali della Sc. Norm. Pisa*, appearing in several parts, 1964-1966.

[C] J. W. S. Cassels : Diophantine equations with special reference to elliptic curves, *J. London Math. Soc.* 41 (1966), 193.

[Co] Fabio Conforto : *Abelsche Functionen und algebraische Geometrie*, Springer, Berlin, 1956.

[D-G] Michel Demazure and Pierre Gabriel : *Séminaire Heidelberg-Strasbourg*.

[G1] Alexandre Grothendieck : *Séminaire de géométrie algébrique*, 1968.

[G2] A. Grothendieck : *Séminaire de géométrie algébrique*, 1960-61.

[G3] A. Grothendieck : *Séminaire de géométrie algébrique*, 1963-64 (Schémas en groupes).

[Go] Roger Godement : *Topologie algébrique et théorie des faisceaux*, Hermann, Paris, 1964.

[G-R] Robert Gunning and Hugo Rossi : *Analytic functions of several complex variables*, Prentice-Hall, 1965.

[H] G. Hochschild : *The structure of Lie groups*, Holden-Day, San Francisco, 1965.

[J] N. JACOBSON : *Lie algebras*, Wiley-Interscience, New York, 1962.

[K] KUNIHIKO KODAIRA : On compact analytic surfaces, *Analytic functions*, Princeton Univ. Press, 1960.

[L] SERGE LANG : *Abelian varieties*, Interscience-Wiley, New York, 1959.

[L-N] SERGE LANG and ANDRÉ NÉRON : Rational points of abelian varieties over function fields, *American J. Math.* 81 (1959), 95.

[M1] DAVID MUMFORD : *Geometric invariant theory*, Springer, Berlin, 1965.

[M2] D. MUMFORD : On the equations defining abelian varieties, *Inv. Math.* 1 (1966), 287.

[M3] D. MUMFORD : *Introduction to algebraic geometry*, forthcoming.

[Ma] YURI MANIN : The theory of commutative formal groups over fields of finite characteristic, *Uspekhi Mat. Nauk.* 18 (1963), No. 6, p. 1; transl. in *Russian Math. Surveys*, Macmillan.

[N] ANDRÉ NÉRON : Modèles minimaux des variétés abeliennes sur les corps locaux et globaux, *Publ. I.H.E.S.* No. 21, 1964.

[O] FRANS OORT : *Commutative group schemes*, Springer Lecture Notes, Vol. 15, 1966.

[S1] J.-P. SERRE : *Groupes algébrique et corps de classes*, Hermann et cie., Paris, 1959.

[Sh] GORO SHIMURA: On analytic families of polarized abelian varieties and automorphic functions, *Annals of Math.* 78 (1963), 149.

[T1] JOHN TATE : p-divisible groups in local fields, *Proc. NUFFIC summer school at Driebergen*, Springer, 1967.

[T2] J. TATE : Endomorphisms of abelian varieties over finite fields, *Inv. Math.* 2 (1966), 134.

[W1] ANDRÉ WEIL : *Variétés abéliennes et courbes algébrique*, Hermann, Paris, 1948.

[W2] A. WEIL : Théorèmes fondamentaux de la théorie des fonctions thêta, *Séminaire Bourbaki*, Exp. 16, 1949.

PRINTED IN INDIA

BY R. SUBBU

AT THE

TATA PRESS LIMITED

BOMBAY

AND

PUBLISHED BY

JOHN BROWN

OXFORD UNIVERSITY PRESS

BOMBAY